LifeSize® Transit™ Deployment Guide

September 2010

LifeSize Transit™ Server
LifeSize Transit™ Client

September 2010

Copyright Notice

©2005 - 2010 Logitech, and its licensors. All rights reserved.

LifeSize Communications, a division of Logitech has made every effort to ensure that the information contained in this document is accurate and reliable, but assumes no responsibility for errors or omissions. Information in this document is subject to change without notice. Companies, names, and data used in examples herein are fictitious unless noted. This document contains copyrighted and proprietary information which is protected by United States copyright laws and international treaty provisions. No part of the document may be reproduced or transmitted, in any form or by any means, electronic or mechanical, for any purpose, without the express written permission from LifeSize Communications.

Trademark Acknowledgments

LifeSize, the LifeSize logo and other LifeSize marks, are owned by Logitech and may be registered. All other trademarks are the property of their respective owners.

Patent Notice

For patents covering LifeSize® products, refer to lifesize.com/support/legal.

Contacting Technical Services

LifeSize Communications welcomes your comments regarding our products and services. If you have feedback about this or any LifeSize product, please send it to feedback@lifesize.com. Refer to lifesize.com/support for additional ways to contact LifeSize Technical Services.

Welcome to LifeSize Transit

LifeSize Transit enables your video communications devices to communicate across firewalls and Network Address Translation (NAT) devices. Firewalls keep uninvited traffic from entering a network, typically by blocking unsolicited incoming requests, including calls from video communications devices outside your network. NAT obscures the private IP address of devices behind the firewall usually by mapping the private IP address:port combination of communications coming from these devices to a temporary public IP address and port on the interface connected to the Internet. For video communications devices, this can be problematic, because the private IP addresses of the devices and the various ports that are dynamically determined in a call are buried in the messages exchanged between the devices and may be inaccessible to the NAT.

LifeSize Transit addresses these challenges for SIP and H.323 calls using a client/server approach. LifeSize Transit Server, which typically resides in the DMZ on your network, comprises a unified set of firewall and NAT traversal technologies. It enables firewall and NAT traversal, session and media control for UDP, TCP, and HTTP media, as well as H.460 control. It also serves as an H.323 gatekeeper or SIP proxy and registrar. The LifeSize Transit server is both an H.460 traversal server and a SIP traversal server.

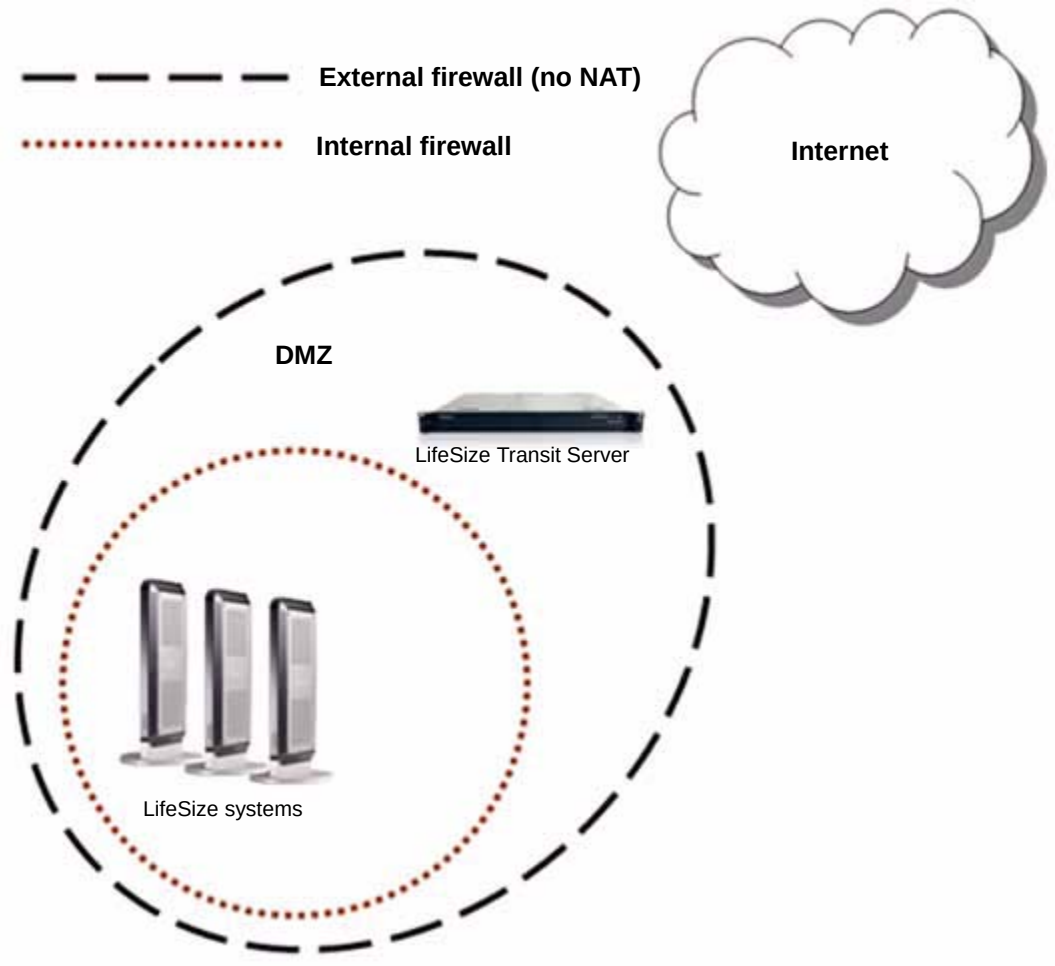
LifeSize video communications systems residing behind the firewall in your private network include client software that enables these devices to register with LifeSize Transit Server. If your LAN includes a supported H.323 gatekeeper, an MCU, or supported third party video communications devices, you can use LifeSize Transit Client—a standalone multi-user traversal client running in your LAN—to serve as a SIP and H.323 proxy for calls with LifeSize Transit Server.

Note: Refer to the *LifeSize Transit Release Notes* for a list of supported third party video communication devices. You must register these devices with the LifeSize Transit Server using LifeSize Transit Client as a SIP and H.323 proxy. Refer to the device manufacturer's documentation to learn how to configure them to use a registrar and proxy.

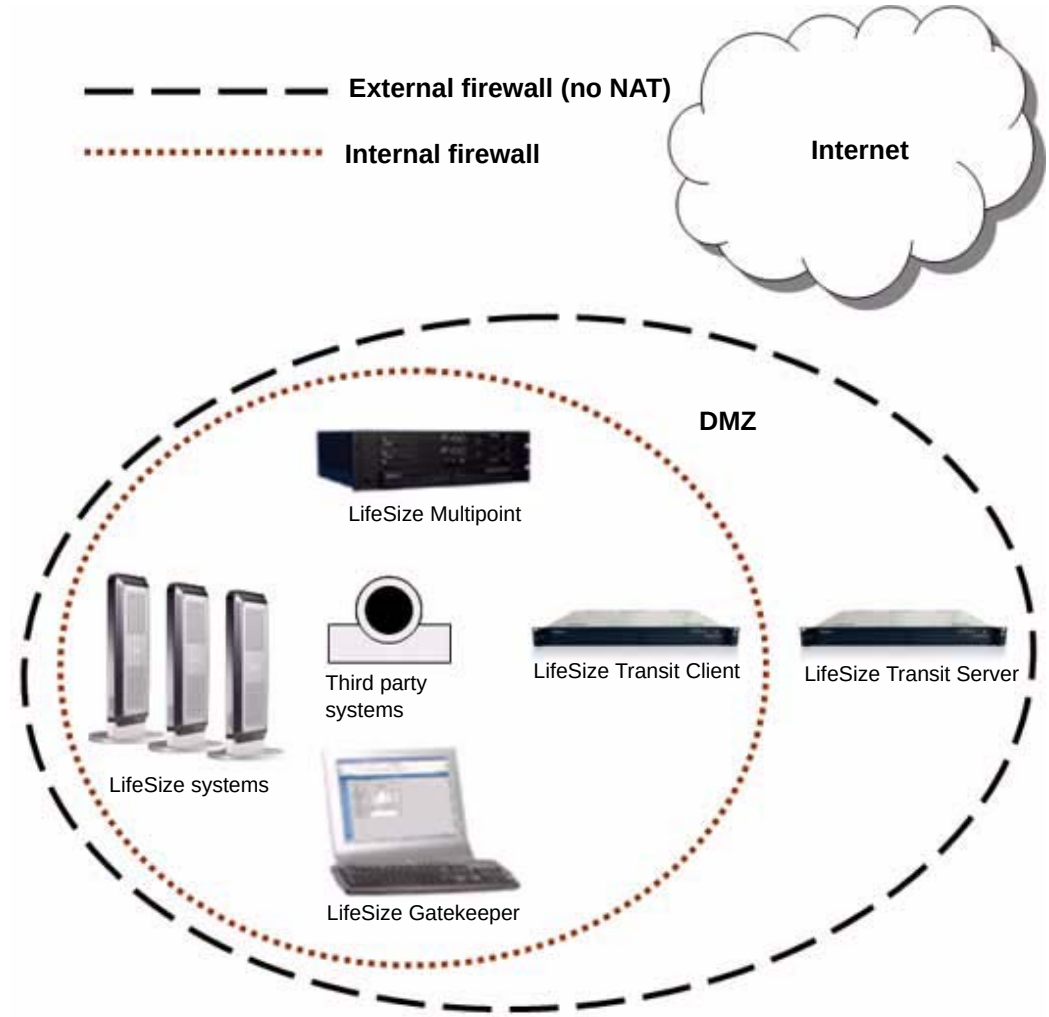
The registration to LifeSize Transit Server, either from LifeSize video communications systems or from the LifeSize Transit Client, creates a connection to the server that is kept alive through small packets that are sent at measured intervals, enabling the server to communicate with the client when it receives an incoming call. The client can then initiate outbound connections on the firewall.

The following diagrams illustrate these deployment options.

LifeSize Transit Server Only



LifeSize Transit Server and LifeSize Transit Client



LifeSize Transit Server: How it Works

LifeSize Transit Server includes a signaling server that handles firewall and NAT traversal, call setup, operation and maintenance services and a media server that is optimized for relaying the actual voice, video, and application sharing data. When you install LifeSize Transit Server, you configure each of these servers with its own static, public IP address. The public IP address of the signaling server is used by callers outside your network to place calls to your video communications devices.

Deploying LifeSize Transit for SIP Calls

If you configure LifeSize Transit for traversal of SIP calls, you must configure a SIP domain on LifeSize Transit Server. To configure your SIP domain to be reachable from other clients or other SIP servers, you must also set up SIP DNS SRV records. Refer to “Creating SIP Domains and DNS SRV Records” on page 17.

LifeSize Transit Server includes a SIP registrar that stores user registrations and handles authentication. You create user accounts on LifeSize Transit Server for each video communications device that will place or receive SIP calls and for LifeSize Transit Client, if included in your deployment. You then use the information from these accounts to configure your video communications devices to register with the SIP registrar on LifeSize Transit Server and use the SIP traversal technologies included in both the client and the server.

Note: Support for using a SIP registrar in the private LAN with LifeSize Transit is not available.

The SIP registrar on LifeSize Transit Server can handle more than one domain at a time and can simultaneously work as a proxy for other SIP users. It can restrict which SIP domains are allowed to register through the server, but does not limit the registered users to place or receive calls from foreign domains.

Traversal for SIP Calls

NAT Traversal for SIP calls with LifeSize Transit Server relies on a suite of protocols: Session Traversal Utilities for NAT (STUN), Traversal Using Relay NAT (TURN), and Interactive Connectivity Establishment (ICE). If NAT traversal using these protocols is not possible, LifeSize Transit Server attempts to use a proprietary method referred to as tunneled mode.

STUN enables your LifeSize devices behind your firewall to discover the public IP address and port mappings that they can use to communicate with other devices during a call and to instruct the other devices where to send media. LifeSize Transit Server comprises a STUN server on both the signaling and media servers.

TURN is an extension of STUN. It allocates a public IP address and port on a server and uses this allocation to relay media between the devices in a call. Both the signalling server and the media server are TURN servers. These relay sessions consume resources on the servers, and, therefore, must be authenticated. The credentials in the **Tunnel** section of the user account that you create in LifeSize Transit Server for each device are used for this authentication. The signalling server handles authentication and authorization of the relay sessions, while the media server performs the actual media relay. To achieve load-sharing of these relay sessions, the traffic requests are redirected to the media server.

ICE is a protocol that makes use of STUN and TURN. It determines the best method for traversal based on a list of transport addresses--a combination of an IP address and UDP port--that each device in a call gathers through STUN, TURN, and from physical or logical network interfaces. ICE is enabled on LifeSize video communications systems by default in **Administrator Preferences : Network : LifeSize Transit** when you configure the devices to use LifeSize Transit for SIP calls.

At start up and at regular intervals thereafter, a LifeSize system that is configured to work with LifeSize Transit probes the network toward LifeSize Transit Server to determine what traversal methods are possible. When these clients connect from NAT using SIP, the public address is noted instead of what is reported from the client. Based on the reported client capabilities, the server decides whether relay is needed when this client participates in a call. The server also makes sure that the signaling channel is kept open while the client is registered.

LifeSize Transit attempts to use the most efficient traversal method in the following order: STUN with ICE, then TURN, and as a last resort the LifeSize proprietary tunneling mode. In tunneled mode, LifeSize Transit Server establishes a tunneled connection to a LifeSize system or the LifeSize Transit Client using TCP port 444 (if available) or TCP port 443.

For information about the ports used for SIP calls with LifeSize Transit, refer to “Configuring Ports for LifeSize Transit” on page 22.

Deploying LifeSize Transit for H.323 Calls

LifeSize Transit supports H.460.18 for H.323 traversal call control and call establishment and H.460.19 for H.323 traversal media control in addition to H.323 on the server side. The deployment consists of the LifeSize Transit Server, which includes an H.460 server, an H.323 gatekeeper, and the clients that you configure to use the server.

To use LifeSize Transit with H.323 calls, you must configure each video communications system with a gatekeeper address. LifeSize Transit can work with a private gatekeeper in the LAN, an external gatekeeper, or use the built-in gatekeeper functionality on LifeSize Transit Server.

Note: In this release, LifeSize Gatekeeper is the only gatekeeper supported in the LAN.

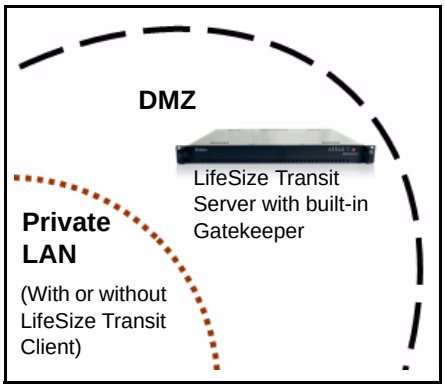
Using the Built-In or an External Gatekeeper

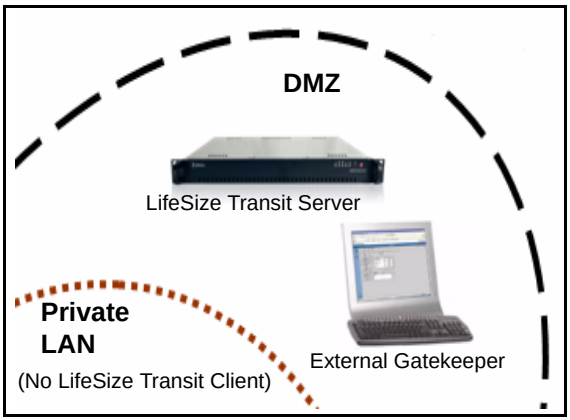
If you are using only LifeSize Transit Server and its built-in gatekeeper or an external gatekeeper, you configure your video communications devices with the signaling server IP address as the gatekeeper address and ensure that H.460 is enabled on the device. With an external gatekeeper, you must also configure LifeSize Transit Server to use the external gatekeeper. You can choose the gatekeeper option that applies to your deployment from the H.323 Configuration page in the LifeSize Transit Server web administration interface. When

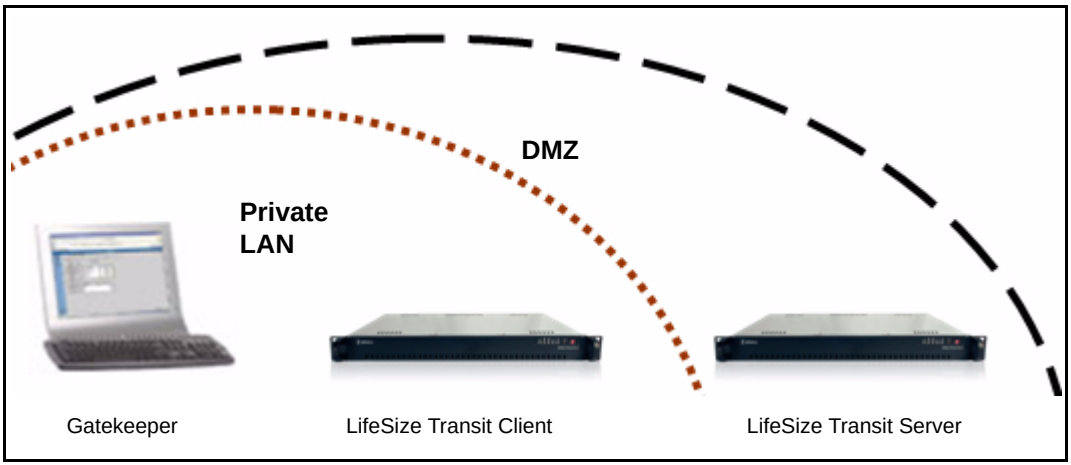
you choose the option to use an external gatekeeper, you specify the IP address and vendor of the external gatekeeper. Refer to “H.323 Configuration” on page 66 for more information about these options.

If you are using LifeSize Transit Client with the built-in gatekeeper in LifeSize Transit Server, you configure the connection between the LifeSize Transit Client and the server and then configure your video communications systems to use the IP address of LifeSize Transit Client as the gatekeeper address. Because traversal is handled by the LifeSize Transit Client in this configuration, ensure that H.460 is not enabled on the video communications devices.

LifeSize Transit Server Mutually Exclusive Gatekeeper Options







Using a Gatekeeper in the Private LAN

When you use a supported gatekeeper in the private LAN, you must use LifeSize Transit Client. All video communications devices and LifeSize Transit Client must register to the same private gatekeeper in the LAN.

Following is an overview of the configuration tasks required for this deployment scenario. For detailed configuration instructions, refer to “Deploying LifeSize Transit Client with a Private Gatekeeper” on page 34.

1. Configure LifeSize Transit Server to use the private gatekeeper in the LAN.
2. Configure the connection between LifeSize Transit Client and LifeSize Transit Server.
3. Create a route on LifeSize Transit Server for sending incoming calls to the private gatekeeper through LifeSize Transit Client.
4. Configure an outbound prefix on LifeSize Transit Client for routing outbound calls. When LifeSize Transit Client registers to the gatekeeper, this prefix automatically becomes a user-defined service prefix on the gatekeeper, making it possible to route outbound H.323 calls from video communications device in the LAN to LifeSize Transit Client.
5. Register Transit Client to the gatekeeper.
6. Configure video communications devices to register with the gatekeeper in the LAN by specifying the prefix for the incoming route that you configured on LifeSize Transit Server as the prefix of the H.323 extension for the device. Also ensure that H.460 is not enabled on the device.

For information about the ports used for H.323 and H.460, refer to ”Configuring Ports for LifeSize Transit” on page 22.

Preparing for a LifeSize Transit Deployment

This guide assumes that you are an administrator who is responsible for configuring, maintaining, and troubleshooting video communications devices that use SIP or H.323 protocols on your network and that you have a working knowledge of the supporting infrastructure (for example, SIP domains, SRV records, SIP registrars, and H.323 gatekeepers) that may be required to deploy these devices.

This guide describes how LifeSize Transit handles firewall traversal for SIP and H.323 calls, the configuration options available, and the associated tasks that you must perform to deploy the product. Configuration instructions throughout this guide identify the specific protocol to which they apply. If you are using both SIP and H.323 protocols for video communications, ensure that you complete the configuration tasks applicable to each protocol and the deployment option that you choose. By default, both protocols are enabled

on LifeSize video communications systems. Refer to your LifeSize video communications systems technical documentation for information about enabling or disabling these protocols.

Planning is essential to successfully deploying network infrastructure devices and solutions. To avoid unexpected problems and to stay on schedule, LifeSize recommends a phased approach to deploying LifeSize Transit that includes planning, installing, configuring, testing, and training IT staff before going live. Use the information in the following sections to prepare a LifeSize Transit deployment plan for your organization.

Deployment Overview

Deploying LifeSize Transit includes the following tasks.

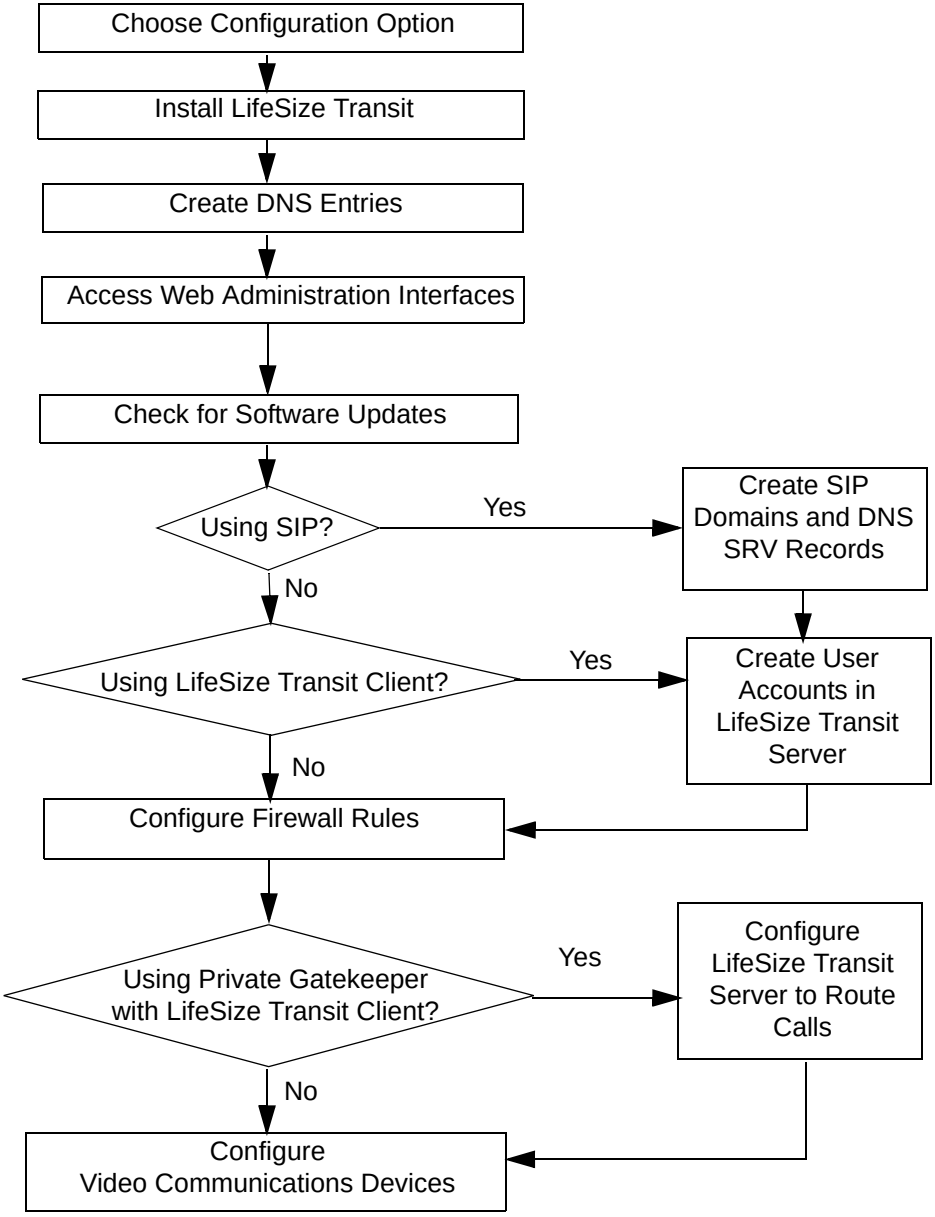
> ***Note:*** If you are adding LifeSize Transit Client to an existing deployment, refer to "Deploying LifeSize Transit Client in an Existing Installation" on page 13.

1. Choose a configuration option. Refer to "LifeSize Transit Configurations" on page 14.
2. Install LifeSize Transit. Refer to "Installation Requirements" on page 15.
3. Create DNS entries. Refer to "DNS Entries" on page 15.
4. Ensure that you can access the web administration interface of LifeSize Transit Server and, if installed, LifeSize Transit Client from a supported web browser in your private network. Refer to "Accessing the Web Administration Interface" on page 16. Refer to the *LifeSize Transit Release Notes* for a list of supported web browsers.
5. Check for software updates and upgrade LifeSize Transit. Refer to "Upgrading Software" on page 47.
6. If you are placing or receiving SIP calls with your video communications systems:
   a. Create SIP domains and DNS SRV RR records. Refer to "Creating SIP Domains and DNS SRV Records" on page 17.
   b. Create a user account in LifeSize Transit Server for each video communications system and MCU in your private network. Refer to "Managing User Accounts" on page 18.

   Note: MCUs are supported only in the private LAN with Transit Client.
7. Create a user account for LifeSize Transit Client if included in your installation. Refer to "Managing User Accounts" on page 18.
8. Configure firewall settings to enable communication between the clients in your private network and LifeSize Transit Server in the DMZ. Refer to "Configuring Ports for LifeSize Transit" on page 22.

9. If you are using a gatekeeper in the private network with LifeSize Transit Client, configure LifeSize Transit Server to route calls through LifeSize Transit Client to the gatekeeper. Refer to ”Deploying LifeSize Transit Client with a Private Gatekeeper” on page 34.
10. Configure the video communications devices in your private network to use LifeSize Transit. Refer to ”Configuring LifeSize Systems for Firewall Traversal” on page 37.
11. Test the installation by placing and monitoring calls. Instructions appear in each section in this manual that describes how to configure LifeSize video communications systems.

The following diagram shows the high-level tasks and dependencies involved in deploying LifeSize Transit.


Choose Configuration Option
Install LifeSize Transit
Create DNS Entries
Access Web Administration Interfaces
Check for Software Updates
Using SIP?
Yes
Create SIP Domains and DNS SRV Records
No
Using LifeSize Transit Client?
Yes
Create User Accounts in LifeSize Transit Server
No
Configure Firewall Rules
Using Private Gatekeeper with LifeSize Transit Client?
Yes
Configure LifeSize Transit Server to Route Calls
No
Configure Video Communications Devices

Use the following checklist to assist you in preparing for a LifeSize Transit deployment:

- ☐ Which video communications protocols are used in the network?

  __SIP __H.323 __Both

- ☐ List the makes, models, IP addresses, and software versions of the video communications systems you intend to use. Refer to the *LifeSize Transit Release Notes* for third party interoperability and supported software versions.

- ☐ List the makes, models, IP addresses, and supported software versions if any, of the MCUs that you intend to use. Refer to the *LifeSize Transit Release Notes* for third party interoperability and supported software versions.

- ☐ Do you plan to use LifeSize Gatekeeper in the private LAN with LifeSize Transit Client?

  __Yes __No

- ☐ Is LifeSize Desktop deployed in your organization?

  __Yes __No

Deploying LifeSize Transit Client in an Existing Installation

If you have an existing LifeSize Transit deployment and are adding LifeSize Transit Client to your network, complete the following tasks:

1. Install LifeSize Transit Client as either a physical device or as a virtual appliance. Refer to ”Installation Requirements” on page 15.
2. Ensure that you can access the web administration interface of LifeSize Transit Client. Refer to ”Accessing the Web Administration Interface” on page 16.
3. Locate the software version of the client on the main page of the web administration interface. Compare the version to the most recent version available on lifesize.com/support and upgrade the client, if needed. Refer to ”Upgrading to the Latest Software Release” on page 16.
4. Ensure that LifeSize Transit Server is installed with a compatible software version. Refer to the *LifeSize Transit Release Notes* on lifesize.com/support.
5. Create a user account for LifeSize Transit Client. Refer to ”Managing User Accounts” on page 18.
6. Modify firewall rules. Refer to ”Configuring Ports for LifeSize Transit” on page 22.
7. If your video communications devices use H.323, and you intend to use a supported gatekeeper in your private network with LifeSize Transit Client, complete the configuration instructions in ”Deploying LifeSize Transit Client with a Private Gatekeeper” on page 34.

8. Modify the configuration of your video communications devices to use the LifeSize Transit Client and test the modifications:
   - For SIP calls, refer to ”Configuring LifeSize Devices for SIP with LifeSize Transit Client” on page 40.
   - For H.323 calls with LifeSize Transit Client and a private gatekeeper, refer to ”Configuring LifeSize Devices for H.323 with LifeSize Transit Client and a Private Gatekeeper” on page 43.
   - For LifeSize Transit Client and the built in gatekeeper on LifeSize Transit Server, refer to ”Configuring LifeSize Devices for H.323 with LifeSize Transit Client and Built-In Gatekeeper” on page 44.

LifeSize Transit Configurations

You can deploy LifeSize Transit in one of the following ways:

Option 1: Deploying LifeSize Transit Server Only

Install only LifeSize Transit Server if your network meets **all** of the following conditions:

- You are using only LifeSize video communications systems behind the firewall in your private network.
- An MCU or H.323 gatekeeper does not exist in your private network.

Option 2: Deploying LifeSize Transit Server with LifeSize Transit Client

Install LifeSize Transit Server and LifeSize Transit Client if your network meets **any** of the following conditions:

- You are using third party video communications devices.
- A supported MCU and/or H.323 gatekeeper exists in your private network. Refer to the *LifeSize Transit Release Notes* for a list of supported MCUs and H.323 gatekeepers with LifeSize Transit Client. This document is available at lifesize.com/support.

Note: LifeSize recommends that if you deploy LifeSize Transit Client, that you configure all devices, including LifeSize video communications systems to use Lifesize Transit Client.

Installation Requirements

For either configuration option, you must install LifeSize Transit Server. Ensure that this device is located on your network in a publicly addressable subnet that has a direct, non-NAT route to the Internet.

Note: You can place a firewall in front of the LifeSize Transit Server, but it must not be a NAT device.

As part of the installation procedure, and regardless of which protocols (SIP or H.323) your organization uses for video communications, you must configure LifeSize Transit Server with two static public IP addresses—one for the signaling server and one for the media server.

You must also configure LifeSize Transit Server with the IP addresses of a primary and, optionally, a secondary DNS server as a backup. These servers can be public DNS servers.

Note: LifeSize Transit Server fails to function properly if it is not configured to use a valid, available DNS server.

If you plan to deploy LifeSize Transit Client, it must be located behind your firewall in the private network in the same LAN as the devices that you intend to use with it. During the installation procedure, configure LifeSize Transit Client with a static private IP address.

Note: Configuration settings in LifeSize Transit and in video communications systems configured to use LifeSize Transit Client in most of the deployment scenarios described in this guide, and firewall rules configured for use with LifeSize Transit Client rely on this IP address.

For detailed installation instructions, refer to the *LifeSize Transit Installation Guide*. If you plan to install LifeSize Transit Client as a virtual appliance, refer to the *LifeSize Transit Client Virtual Appliance Installation Guide*. The *LifeSize Transit Installation Guide* is available on the documentation CD included in the product box and at lifesize.com/support. The *LifeSize Transit Client Virtual Appliance Installation Guide* is available at lifesize.com/support.

DNS Entries

For LifeSize Transit Server to be publicly accessible, the signalling and media servers need to have public addresses that are registered in the global DNS service. If your organization does not manage its domain names, ask your Internet Service Provider (ISP) to do this. The DNS entries chosen for the servers must match the name in the SSL certificate. For example:

- `pxs1.example.com` for the signalling server
- `me1.example.com` for the media server

Accessing the Web Administration Interface

After you install LifeSize Transit and configure DNS entries, ensure that you can connect to the web administration interface of LifeSize Transit Server from a supported web browser in your private network. For a list of supported web browsers, refer to the *LifeSize Transit Release Notes*.

> ***Note:*** You must allow access to TCP ports 8080 and 8181 on LifeSize Transit Server. LifeSize recommends that you provide this access only to systems behind the firewall or NAT in the private LAN.

1. Enter the IP address or fully qualified domain name of the signalling server plus port 8181 on HTTPS. For example:

   `https://`*`transitserver.example.com`*`:8181`

2. Enter the LifeSize Transit administrator username and password. The default value for both is *admin*.

   > ***Note:*** You can change these values from the initial configuration screen as described in the *LifeSize Transit Installation Guide*.

3. Ensure that you can access the software upgrade or additional maintenance task pages through port 8080. On the **Operation & Maintenance** menu, click either **Software Upgrade** or **Additional Maintenance Tasks**. If prompted for a username and password, enter the LifeSize Transit administrator username and password. The default value for both is *admin*. The IP address of the signaling server followed by `:8080` appears in the address field of your browser.

4. If you installed LifeSize Transit Client, ensure that you can access its web administration interface. In a supported browser, enter the IP address of LifeSize Transit Client. Enter the username and password in the login dialog box that appears. The default is `admin` for both. You can change these credentials in the initial configuration screen. Refer to the *LifeSize Transit Installation Guide*, or if you installed LifeSize Transit Client as a virtual appliance, the *LifeSize Transit Client Virtual Appliance Installation Guide*.

Upgrading to the Latest Software Release

After you ensure that you can access the web administration interface of LifeSize Transit Server and LifeSize Transit Client, check for software updates. Refer to ”Upgrading Software” on page 47.

> ***Note:*** Ensure that LifeSize Transit Server and LifeSize Transit Client are installed with compatible software releases. Refer to the *LifeSize Transit Release Notes*.

Refer to the *LifeSize Transit Release Notes* for the software version of LifeSize and third party devices that are supported with the version of LifeSize Transit that you are using and upgrade these devices, if needed.

Creating SIP Domains and DNS SRV Records

If you are planning to place or receive SIP calls with your video communications devices, use the information in this section to ensure that your environment is configured properly to work with LifeSize Transit. By default, SIP is enabled on LifeSize video communications systems in **Administrator Preferences : Communications : SIP**.

Configuring SIP Domains

You must configure a SIP domain name to use the LifeSize Transit Server for SIP calls. To configure a SIP domain, follow these steps:

1. Access the web administration interface for LifeSize Transit Server. Refer to ”Accessing the Web Administration Interface” on page 16.
2. On the **Operation & Maintenance** menu, click **SIP Registrar Settings**.
3. Under **SIP Domains**, enter your SIP domain name.
4. Click the **+** button to add the domain.

   Note: For more information about this page, refer to ”SIP Registrar Settings” on page 62.

Configuring DNS SRV Records for SIP

To configure your SIP domain to be reachable from other clients or other SIP servers, you may set up a SIP DNS SRV record, so that external systems do not need to be configured with the IP address of LifeSize Transit Server. If all calls go through the LifeSize Transit Server or LifeSize devices, your SIP domain does not have to resolve through DNS.

The signaling server on LifeSize Transit Server acts as the registrar for the particular domain(s). Use its IP address as the target in SIP SRV records. A typical SIP SRV RR for the registrar at domain example.com looks like this:

_Service._Proto.Name	TTL	Class	Priority	Weight	Port	Target
_sip._udp.example.com		IN	0	0	5060	*Signaling server IPaddress*
_sip._tcp.example.com		IN	0	0	5060	*Signaling server IPaddress*

Managing User Accounts

A tunneled SIP connection or media that is relayed in SIP calls with LifeSize Transit Server consumes resources on the server and, therefore, requires user authentication. Another set of credentials is also required when a device registers with the SIP registrar in LifeSize Transit Server. A user account in LifeSize Transit Server contains both sets of credentials. Use the instructions in this section to create a user account for each video communications device and MCU that places or receives SIP calls. You must also create a user account for each LifeSize Desktop installation that you intend to use with LifeSize Transit.

Regardless of the protocols used on your network for video communication, you must create a user account for LifeSize Transit Client, if it is included in the deployment.

When you create these accounts, if you are using LifeSize Transit Server only, make note of the **User ID** and **Password** that you enter in the **Tunnel** section and the **SIP Digest Username** and **Password** in the **SIP and H.323** section of the **Create New User Account** page. The credentials in the **Tunnel** section of the page are for authenticating the user for a tunneled connection to the server. You will need these credentials when you later configure LifeSize video communications devices to use the SIP traversal portion of the client software on the device. The SIP credentials in the **SIP and H.323** section of the page are for authenticating the connection between the video communications device and the SIP registrar in LifeSize Transit Server. You use these credentials when you later configure LifeSize video communications devices to register to the SIP registrar.

If you are using LifeSize Transit Client, for each user account that you create for a video communications device, make note of the **SIP Digest Username** and **Password** in the **SIP and H.323** section of the **Create New User Account** page. You will need these values later when you configure these devices to register to the SIP registrar. Although the credentials in the **Tunnel** section of the page are required to create the user account, these credentials are not used by video communications devices when LifeSize Transit Client is included in the deployment.

Only the tunnel credentials in the user account for the LifeSize Transit Client are used for the connection to LifeSize Transit Server when LifeSize Transit Client is deployed. Therefore, when you create the user account for LifeSize Transit Client, make note of the credentials that you enter in the **Tunnel** section of the **Create New User Account** page. You use these credentials later when you configure LifeSize Transit Client to connect to LifeSize Transit Server. Fields in the **SIP and H.323** section of the page that are required to create a user account for the LifeSize Transit Client are not used.

User accounts are stored in the LifeSize Transit Server database. For more information about the database, refer to ”Database Configuration” on page 58. To back up or restore the database, refer to ”Database Backup and Restore” on page 46.

Creating User Accounts

Follow these steps to create a user account for each video communications system, MCU, and LifeSize Transit Client, if applicable to your environment:

1. Access the LifeSize Transit Server web administration interface.
2. On the **Provisioning** menu, click **Create User**.
3. Enter the information for the new user account. Required fields are indicated with an asterisk (*).

   Note: Entries must not contain spaces. Only the following characters are valid:

   - alphanumeric (A-Z, a-z, and 0-9)
   - . (period)
   - _ (underscore)
   - - (dash)
   - ~ (tilde)
   - @ (SIP ID only. Do not use in any other field.)

The following table describes the required and optional fields in the **Tunnel** and **SIP and H.323** sections of the page. The fields in the **Optional Information** section of the page include the name and contact information for the user.

Note: Only the tunnel user ID and password are used by LifeSize Transit Server for the LifeSize Transit Client user account. You must supply values for all required fields to create the record.

Label	Description
Tunnel:	
User ID	Required field. The user ID for the LifeSize Transit user. The maximum length is 50 characters.
Password	Required field. The password for the LifeSize Transit user. Maximum length is 50 characters.

Label	Description
SIP and H.323:	
SIP ID	Required field. The user's SIP ID. (For example, user@sipdomain.com) Maximum length is 50 characters.
SIP Digest User Name	Required field. Usually this is the user name part of the SIP ID (for example *user* for the SIP ID *user@sipdomain.com*). (On LifeSize systems that are configured for SIP, this is the same as the **SIP Username** in **Administrator Preferences : Communications : SIP**) At least 4, but not to exceed 50 characters in length.
SIP Alias	An alias used to refer to the SIP user. Maximum length is 50 characters.
H.323 User Alias	An alias used to refer to the H.323 user. Maximum length is 50 characters.
H.323 User Number	The user's H.323 ID. Maximum length is 50 characters.
Password	Required field The SIP authorization password. (On Lifesize systems that are configured for SIP, this is the **Authorization Password** in **Administrator Preferences : Communications : SIP**) Maximum length is 50 characters.

4. Click **Add**.
5. After you create an account, ensure that it appears on the **User accounts** page in LifeSize Transit Server. On the **Provisioning** menu, click **List Users** to list the following information for all user accounts in the database:

Label	Description
ID	The internal ID for the LifeSize Transit user.
Name	The name of the LifeSize Transit user as entered in the optional **Full Name** field in the **Create New User Account** page.

Label	Description
Country	The country for the LifeSize Transit user as entered in the optional **Country** field in the **Create New User Account** page.
E-mail	The email address for the LifeSize Transit user as entered in the optional **E-mail** field in the **Create New User Account** page.
Phone	The phone number for the LifeSize Transit user as entered in the optional **Phone** field in the **Create New User Account** page.
Login ID	The value entered in the **User ID** field of the **Tunnel** section on the **Create New User Account** page.
SIP ID	The user's SIP ID.
SIP User Name	The value entered in the **SIP Digest User Name** field on the **Create New User Account** page.
SIP Alias	An alias used to refer to the SIP user.
H.323 Alias	An alias used to refer to the H.323 user.
H.323 Number	The user's H.323 ID.
Lock	Prevents the user from accessing the system.

Modifying or Deleting a User Account

You can modify or delete a user account from the **User Accounts** page by clicking **Edit** in the entry for the user. Click **Update** or **Add** after making changes. Click **Delete** to remove the entire user account.

Searching for User Accounts

You can search for users by name, email address, LifeSize Transit Server ID, or SIP/H.323 ID. Click **Search Users** from the **Provisioning** menu.

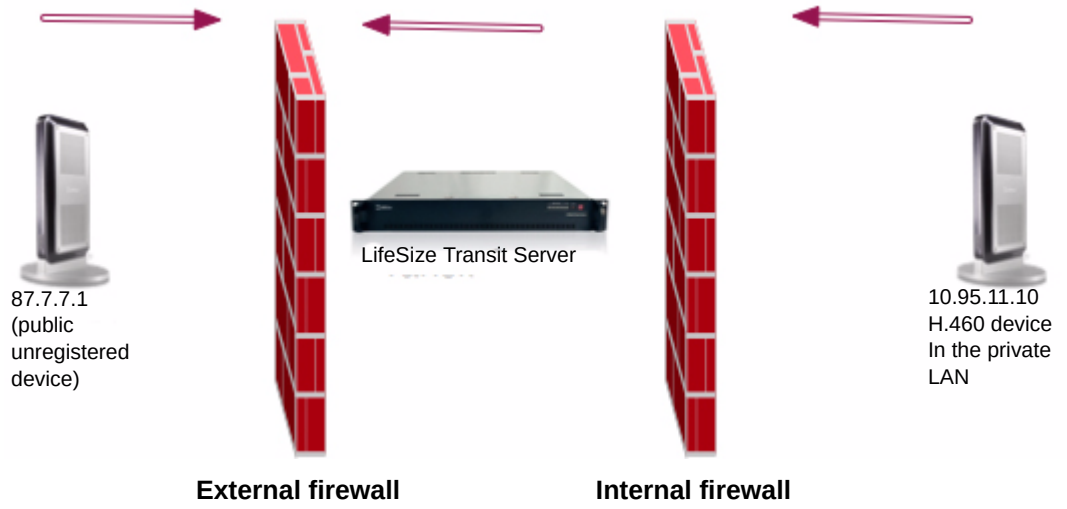
Configuring Ports for LifeSize Transit

You must add rules to your firewall to allow inbound traffic from any IP address and port to the ports listed in the following tables as well as rules to allow outbound traffic from the ports listed in the following tables to any IP address and port. Each table is followed by an example of a full set of firewall rules for using a particular protocol with LifeSize Transit.

Note: **The example firewall rules assume that the firewall is configured to allow return traffic on any allowed connection.** LifeSize recommends turning off any H.323 and SIP fix up protocols, if possible, as these can cause problems in cases where they are not updated to the latest versions of the H.323 and SIP standards.

The example rules that follow each table identify rules for both an external firewall and an internal firewall. The external firewall is one placed in front of LifeSize Transit Server facing the Internet. The internal firewall is one placed between LifeSize Transit Server and devices on the private network. The inbound direction is always from the Internet to the private network. The outbound direction is always from the private network to the Internet

.



Configuring Ports for SIP

To use standards-based SIP, enable the ports listed in the following table for LifeSize Transit Server. Refer to the example set of firewall rules that follow the table.

	Signaling Server TCP	Signaling Server UDP	Media Server TCP	Media Server UDP
Basic SIP	5060	5060		
STUN		3478, 34501		3478, 34501
TURN	3560	3560	3560	3560
RTP/Media				45100-46699

Note: The media server port ranges have expanded in this release. Ensure that your firewall is adjusted to account for this.

Firewall Rules for SIP with LifeSize Transit

The following is an example set of firewall rules for using SIP/STUN/TURN/RTP with LifeSize Transit Server.

The following rules apply to the external firewall as inbound rules, whether you are using LifeSize Transit Server alone or in conjunction with LifeSize Transit Client:

Allow SRC_IP=any	SRC_PORT=any	DST_IP=SignalingIP	DST_PORT=5060tcp
Allow SRC_IP=any	SRC_PORT=any	DST_IP=SignalingIP	DST_PORT=5060udp
Allow SRC_IP=any	SRC_PORT=any	DST_IP=SignalingIP	DST_PORT=3478udp
Allow SRC_IP=any	SRC_PORT=any	DST_IP=SignalingIP	DST_PORT=34501udp
Allow SRC_IP=any	SRC_PORT=any	DST_IP=SignalingIP	DST_PORT=3560tcp
Allow SRC_IP=any	SRC_PORT=any	DST_IP=SignalingIP	DST_PORT=3560udp
Allow SRC_IP=any	SRC_PORT=any	DST_IP=MediaIP	DST_PORT=3478udp
Allow SRC_IP=any	SRC_PORT=any	DST_IP=MediaIP	DST_PORT=34501udp
Allow SRC_IP=any	SRC_PORT=any	DST_IP=MediaIP	DST_PORT=3560tcp

Allow SRC_IP=any	SRC_PORT=any	DST_IP=MediaIP	DST_PORT=3560udp
Allow SRC_IP=any	SRC_PORT=any	DST_IP=MediaIP	DST_PORT=45100-46699udp

The following rules apply to the internal firewall as outbound rules ***if you are using LifeSize Transit Server only***. Skip to the next set of rules for the internal firewall if you are using LifeSize Transit Client.

Allow SRC_IP=any	SRC_PORT=any	DST_IP=SignalingIP	DST_PORT=5060tcp
Allow SRC_IP=any	SRC_PORT=any	DST_IP=SignalingIP	DST_PORT=5060udp
Allow SRC_IP=any	SRC_PORT=any	DST_IP=SignalingIP	DST_PORT=3478udp
Allow SRC_IP=any	SRC_PORT=any	DST_IP=SignalingIP	DST_PORT=34501udp
Allow SRC_IP=any	SRC_PORT=any	DST_IP=SignalingIP	DST_PORT=3560tcp
Allow SRC_IP=any	SRC_PORT=any	DST_IP=SignalingIP	DST_PORT=3560udp
Allow SRC_IP=any	SRC_PORT=any	DST_IP=MediaIP	DST_PORT=3478udp
Allow SRC_IP=any	SRC_PORT=any	DST_IP=MediaIP	DST_PORT=34501udp
Allow SRC_IP=any	SRC_PORT=any	DST_IP=MediaIP	DST_PORT=3560tcp
Allow SRC_IP=any	SRC_PORT=any	DST_IP=MediaIP	DST_PORT=3560udp
Allow SRC_IP=any	SRC_PORT=any	DST_IP=MediaIP	DST_PORT=45100-46699udp

The following rules apply to the internal firewall as outbound rules ***if you are using LifeSize Transit Client*** (TC):

Allow SRC_IP=TC_IP	SRC_PORT=any	DST_IP=SignalingIP	DST_PORT=5060tcp
Allow SRC_IP=TC_IP	SRC_PORT=any	DST_IP=SignalingIP	DST_PORT=5060udp
Allow SRC_IP=TC_IP	SRC_PORT=any	DST_IP=SignalingIP	DST_PORT=3478udp
Allow SRC_IP=TC_IP	SRC_PORT=any	DST_IP=SignalingIP	DST_PORT=34501udp

Allow SRC_IP=TC_IP	SRC_PORT=any	DST_IP=SignalingIP	DST_PORT=3560tcp
Allow SRC_IP=TC_IP	SRC_PORT=any	DST_IP=SignalingIP	DST_PORT=3560udp
Allow SRC_IP=TC_IP	SRC_PORT=any	DST_IP=MediaIP	DST_PORT=3478udp
Allow SRC_IP=TC_IP	SRC_PORT=any	DST_IP=MediaIP	DST_PORT=34501udp
Allow SRC_IP=TC_IP	SRC_PORT=any	DST_IP=MediaIP	DST_PORT=3560tcp
Allow SRC_IP=TC_IP	SRC_PORT=any	DST_IP=MediaIP	DST_PORT=3560udp
Allow SRC_IP=TC_IP	SRC_PORT=any	DST_IP=MediaIP	DST_PORT=45100-46699udp

The following rules apply to the external firewall as outbound rules, whether you are using LifeSize Transit Server alone or in conjunction with LifeSize Transit Client:

Allow SRC_IP=SignalingIP	SRC_PORT=5060udp	DST_IP=any	DST_PORT=any
Allow SRC_IP=SignalingIP	SRC_PORT=3478udp	DST_IP=any	DST_PORT=any
Allow SRC_IP=SignalingIP	SRC_PORT=34501udp	DST_IP=any	DST_PORT=any
Allow SRC_IP=SignalingIP	SRC_PORT=3560udp	DST_IP=any	DST_PORT=any
Allow SRC_IP=SignallingIP	SRC_PORT=anytcp	DST_IP=any	DST_PORT=any
Allow SRC_IP=MediaIP	SRC_PORT=3478udp	DST_IP=any	DST_PORT=any
Allow SRC_IP=MediaIP	SRC_PORT=34501udp	DST_IP=any	DST_PORT=any
Allow SRC_IP=MediaIP	SRC_PORT=3560tcp	DST_IP=any	DST_PORT=any
Allow SRC_IP=MediaIP	SRC_PORT=3560udp	DST_IP=any	DST_PORT=any
Allow SRC_IP=MediaIP	SRC_PORT=45100-46699udp	DST_IP=any	DST_PORT=any

The following rules apply to the internal firewall as inbound rules ***if you are using LifeSize Transit Server only***. Skip to the next set of rules for the internal firewall if you are using LifeSize Transit Client.

Allow SRC_IP=SignalingIP	SRC_PORT=5060tcp	DST_IP=any	DST_PORT=any
Allow SRC_IP=SignalingIP	SRC_PORT=5060udp	DST_IP=any	DST_PORT=any
Allow SRC_IP=SignalingIP	SRC_PORT=3478udp	DST_IP=any	DST_PORT=any
Allow SRC_IP=SignalingIP	SRC_PORT=34501udp	DST_IP=any	DST_PORT=any
Allow SRC_IP=SignalingIP	SRC_PORT=3560tcp	DST_IP=any	DST_PORT=any
Allow SRC_IP=SignalingIP	SRC_PORT=3560udp	DST_IP=any	DST_PORT=any
Allow SRC_IP=MediaIP	SRC_PORT=3478udp	DST_IP=any	DST_PORT=any
Allow SRC_IP=MediaIP	SRC_PORT=34501udp	DST_IP=any	DST_PORT=any
Allow SRC_IP=MediaIP	SRC_PORT=3560tcp	DST_IP=any	DST_PORT=any
Allow SRC_IP=MediaIP	SRC_PORT=3560udp	DST_IP=any	DST_PORT=any
Allow SRC_IP=MediaIP	SRC_PORT=45100-46699udp	DST_IP=any	DST_PORT=any

The following rules apply to the internal firewall as inbound rules ***if you are using LifeSize Transit Client*** (TC)

Allow SRC_IP=SignalingIP	SRC_PORT=5060tcp	DST_IP=TC_IP	DST_PORT=any
Allow SRC_IP=SignalingIP	SRC_PORT=5060udp	DST_IP=TC_IP	DST_PORT=any
Allow SRC_IP=SignalingIP	SRC_PORT=3478udp	DST_IP=TC_IP	DST_PORT=any
Allow SRC_IP=SignalingIP	SRC_PORT=34501udp	DST_IP=TC_IP	DST_PORT=any
Allow SRC_IP=SignalingIP	SRC_PORT=3560tcp	DST_IP=TC_IP	DST_PORT=any
Allow SRC_IP=SignalingIP	SRC_PORT=3560udp	DST_IP=TC_IP	DST_PORT=any
Allow SRC_IP=MediaIP	SRC_PORT=3478udp	DST_IP=TC_IP	DST_PORT=any

Allow SRC_IP=MediaIP	SRC_PORT=34501udp	DST_IP=TC_IP	DST_PORT=any
Allow SRC_IP=MediaIP	SRC_PORT=3560tcp	DST_IP=TC_IP	DST_PORT=any
Allow SRC_IP=MediaIP	SRC_PORT=3560udp	DST_IP=TC_IP	DST_PORT=any
Allow SRC_IP=MediaIP	SRC_PORT=45100-46699udp	DST_IP=TC_IP	DST_PORT=any

Configuring Ports for Tunneled SIP

In SIP calls with LifeSize video communications systems, LifeSize Transit Server attempts to use a tunneled connection between the LifeSize system and the server if all other SIP traversal methods fail. The tunnel is created on TCP port 444 or TCP port 443 (if TCP port 444 is not available).

Note: If you decide not to open port 444, you must allow unencrypted traffic on port 443 or tunneled signalling will fail.

If you are using LifeSize Transit Client, the connection between this client and LifeSize Transit Server is tunneled using these ports. The signaling and the media will be tunneled.

	Signaling Server TCP	**Media Server TCP**
LifeSize Transit tunneled connections	443 and 444	443 and 444

Firewall Rules for LifeSize Transit Tunneled SIP Connections

Following is an example set of firewall rules for using LifeSize Transit tunneled connections between LifeSize Transit clients and LifeSize Transit Server.

The following rules apply to the external firewall as inbound rules:

Allow SRC_IP=any	SRC_PORT=any	DST_IP=SignalingIP	DST_PORT=443tcp
Allow SRC_IP=any	SRC_PORT=any	DST_IP=SignalingIP	DST_PORT=444tcp
Allow SRC_IP=any	SRC_PORT=any	DST_IP=MediaIP	DST_PORT=443tcp
Allow SRC_IP=any	SRC_PORT=any	DST_IP=MediaIP	DST_PORT=444tcp

The following rules apply to the internal firewall as outbound rules ***if you are using LifeSize Transit Server only***. Skip to the next set of rules for the internal firewall if you are using LifeSize Transit Client

Allow SRC_IP=any	SRC_PORT=any	DST_IP=SignalingIP	DST_PORT=443tcp
Allow SRC_IP=any	SRC_PORT=any	DST_IP=SignalingIP	DST_PORT=444tcp
Allow SRC_IP=any	SRC_PORT=any	DST_IP=MediaIP	DST_PORT=443tcp
Allow SRC_IP=any	SRC_PORT=any	DST_IP=MediaIP	DST_PORT=444tcp

The following rules apply to the internal firewall as outbound rules ***if you are using LifeSize Transit Client*** (TC).

Allow SRC_IP=TC_IP	SRC_PORT=any	DST_IP=SignalingIP	DST_PORT=443tcp
Allow SRC_IP=TC_IP	SRC_PORT=any	DST_IP=SignalingIP	DST_PORT=444tcp
Allow SRC_IP=TC_IP	SRC_PORT=any	DST_IP=MediaIP	DST_PORT=443tcp
Allow SRC_IP=TC_IP	SRC_PORT=any	DST_IP=MediaIP	DST_PORT=444tcp

The following rules apply to the external firewall as outbound rules:

Allow SRC_IP=SignalingIP	SRC_PORT=443tcp	DST_IP=any	DST_PORT=any
Allow SRC_IP=SignalingIP	SRC_PORT=444tcp	DST_IP=any	DST_PORT=any
Allow SRC_IP=MediaIP	SRC_PORT=443tcp	DST_IP=any	DST_PORT=any
Allow SRC_IP=MediaIP	SRC_PORT=444tcp	DST_IP=any	DST_PORT=any

The following rules apply to the internal firewall as inbound rules ***if you are using LifeSize Transit Server only***. Skip to the next set of rules for the internal firewall if you are using LifeSize Transit Client.

Allow SRC_IP=SignalingIP	SRC_PORT=443tcp	DST_IP=any	DST_PORT=any
Allow SRC_IP=SignalingIP	SRC_PORT=444tcp	DST_IP=any	DST_PORT=any
Allow SRC_IP=MediaIP	SRC_PORT=443tcp	DST_IP=any	DST_PORT=any
Allow SRC_IP=MediaIP	SRC_PORT=444tcp	DST_IP=any	DST_PORT=any

The following rules apply to the internal firewall as inbound rules ***if you are using LifeSize Transit Client*** (TC).

Allow SRC_IP=SignalingIP	SRC_PORT=443tcp	DST_IP=TC_IP	DST_PORT=any
Allow SRC_IP=SignalingIP	SRC_PORT=444tcp	DST_IP=TC_IP	DST_PORT=any
Allow SRC_IP=MediaIP	SRC_PORT=443tcp	DST_IP=TC_IP	DST_PORT=any
Allow SRC_IP=MediaIP	SRC_PORT=444tcp	DST_IP=TC_IP	DST_PORT=any

Configuring Ports for Tunneled H.323 with LifeSize Transit Client

If you are using LifeSize Transit Client with H.323 calls, the connection between this client and LifeSize Transit Server is tunneled using TCP port 444 or TCP port 443 (if TCP port 444 is not available) if you configure LifeSize Transit Server to use a gatekeeper in the private LAN.

Note: If you decide not to open port 444, you must allow unencrypted traffic on port 443 or tunneled signalling will fail.

For all other gatekeeper configuration options you can configure LifeSize Transit Client to use either a tunneled connection or an H.460.18/19 connection to LifeSize Transit Server.

For H.323 calls that are tunneled with LifeSize Transit Client, the signaling is tunneled, but media will go direct.

	Signaling Server TCP	**Media Server TCP**
LifeSize Transit tunneled connections	443 and 444	443 and 444

Firewall Rules for LifeSize Transit Tunneled H.323 Connections

Following is an example set of firewall rules for using LifeSize Transit tunneled connections between LifeSize Transit clients and LifeSize Transit Server.

The following rules apply to the external firewall as inbound rules:

Allow SRC_IP=any	SRC_PORT=any	DST_IP=SignalingIP	DST_PORT=443tcp
Allow SRC_IP=any	SRC_PORT=any	DST_IP=SignalingIP	DST_PORT=444tcp
Allow SRC_IP=any	SRC_PORT=any	DST_IP=MediaIP	DST_PORT=443tcp
Allow SRC_IP=any	SRC_PORT=any	DST_IP=MediaIP	DST_PORT=444tcp

The following rules apply to the internal firewall as outbound rules.

Allow SRC_IP=TC_IP	SRC_PORT=any	DST_IP=SignalingIP	DST_PORT=443tcp
Allow SRC_IP=TC_IP	SRC_PORT=any	DST_IP=SignalingIP	DST_PORT=444tcp
Allow SRC_IP=TC_IP	SRC_PORT=any	DST_IP=MediaIP	DST_PORT=443tcp
Allow SRC_IP=TC_IP	SRC_PORT=any	DST_IP=MediaIP	DST_PORT=444tcp

The following rules apply to the external firewall as outbound rules:

Allow SRC_IP=SignalingIP	SRC_PORT=443tcp	DST_IP=any	DST_PORT=any
Allow SRC_IP=SignalingIP	SRC_PORT=444tcp	DST_IP=any	DST_PORT=any
Allow SRC_IP=MediaIP	SRC_PORT=443tcp	DST_IP=any	DST_PORT=any
Allow SRC_IP=MediaIP	SRC_PORT=444tcp	DST_IP=any	DST_PORT=any

The following rules apply to the internal firewall as inbound rules:

Allow SRC_IP=SignalingIP	SRC_PORT=443tcp	DST_IP=TC_IP	DST_PORT=any
Allow SRC_IP=SignalingIP	SRC_PORT=444tcp	DST_IP=TC_IP	DST_PORT=any
Allow SRC_IP=MediaIP	SRC_PORT=443tcp	DST_IP=TC_IP	DST_PORT=any
Allow SRC_IP=MediaIP	SRC_PORT=444tcp	DST_IP=TC_IP	DST_PORT=any

Configuring Ports for H.323 and H.460

Enable the ports listed in the following table for LifeSize Transit to use H.323 and H.460. H.323 is appropriate for external systems that are not behind a firewall or NAT.

	TCP Signaling Server	UDP Signaling Server
(H.323 and H.460) H.225	1720	1719
(H.460) H.245	1722	
(H.323) H.245	37000-41105	
(H.460) RTP/Media		6768, 6769
(H.323) RTP/Media		44100-44899

Firewall Rules for LifeSize Transit Using H.323 and H.460

The following is an example set of firewall rules for using H.323 and H.460 with LifeSize Transit Server.

The following rules apply to the external firewall as inbound rules:

Allow SRC_IP=any	SRC_PORT=any	DST_IP=SignalingIP	DST_PORT=1719udp
Allow SRC_IP=any	SRC_PORT=any	DST_IP=SignalingIP	DST_PORT=1720tcp
Allow SRC_IP=any	SRC_PORT=any	DST_IP=SignalingIP	DST_PORT=1722tcp
Allow SRC_IP=any	SRC_PORT=any	DST_IP=SignalingIP	DST_PORT=6768-6769udp
Allow SRC_IP=any	SRC_PORT=any	DST_IP=SignalingIP	DST_PORT=37000-41105tcp
Allow SRC_IP=any	SRC_PORT=any	DST_IP=SignalingIP	DST_PORT=44100-44899udp

The following rules apply to the internal firewall as outbound rules **if you are using LifeSize Transit Server only**. Skip to the next set of rules for the internal firewall if you are using LifeSize Transit Client:.

Allow SRC_IP=any	SRC_PORT=any	DST_IP=SignalingIP	DST_PORT=1720tcp
Allow SRC_IP=any	SRC_PORT=any	DST_IP=SignalingIP	DST_PORT=1722tcp
Allow SRC_IP=any	SRC_PORT=any	DST_IP=SignalingIP	DST_PORT=1719udp
Allow SRC_IP=any	SRC_PORT=any	DST_IP=SignalingIP	DST_PORT=6768-6769udp

The following rules apply to the internal firewall as outbound rules **if you are using LifeSize Transit Client** (TC):

Allow SRC_IP=TC_IP	SRC_PORT=any	DST_IP=SignalingIP	DST_PORT=1720tcp
Allow SRC_IP=TC_IP	SRC_PORT=any	DST_IP=SignalingIP	DST_PORT=1722tcp
Allow SRC_IP=TC_IP	SRC_PORT=any	DST_IP=SignalingIP	DST_PORT=1719udp
Allow SRC_IP=TC_IP	SRC_PORT=any	DST_IP=SignalingIP	DST_PORT=6768-6769udp

The following rules apply to the external firewall as outbound rules:

Allow SRC_IP=SignalingIP	SRC_PORT=1719udp	DST_IP=any	DST_PORT=any
Allow SRC_IP=SignalingIP	SRC_PORT=44100-44899udp	DST_IP=any	DST_PORT=any
Allow SRC_IP=SignallingIP	SRC_PORT=anytcp	DST_IP=any	DST_PORT=any

The following rules apply to the internal firewall as inbound rules **if you are using LifeSize Transit Server only**. Skip to the next set of rules for the internal firewall if you are using LifeSize Transit Client.

Allow SRC_IP=SignalingIP	SRC_PORT=1720tcp	DST_IP=any	DST_PORT=any
Allow SRC_IP=SignalingIP	SRC_PORT=37000-41105tcp	DST_IP=any	DST_PORT=any
Allow SRC_IP=SignalingIP	SRC_PORT=1719udp	DST_IP=any	DST_PORT=any
Allow SRC_IP=SignalingIP	SRC_PORT=44100-44899udp	DST_IP=any	DST_PORT=any

The following rules apply to the internal firewall as inbound rules ***if you are using LifeSize Transit Client***.

Allow SRC_IP=SignalingIP	SRC_PORT=1720tcp	DST_IP=TC_IP	DST_PORT=any
Allow SRC_IP=SignalingIP	SRC_PORT=37000-41105tcp	DST_IP=TC_IP	DST_PORT=any
Allow SRC_IP=SignalingIP	SRC_PORT=1719udp	DST_IP=TC_IP	DST_PORT=any
Allow SRC_IP=SignalingIP	SRC_PORT=44100-44899udp	DST_IP=TC_IP	DST_PORT=any

Configuring Ports for LifeSize Transit Server Web Administration

To allow access to the web administration interface of LifeSize Transit Server, you must allow access to TCP ports 8080 and 8081 on LifeSize Transit Server. LifeSize recommends that you provide this access only to systems behind the firewall or NAT. For more information about accessing the web administration interface, refer to “Accessing the Web Administration Interface” on page 16.

Deploying LifeSize Transit Client with a Private Gatekeeper

If you are using a supported H.323 gatekeeper in your private network with LifeSize Transit Client, complete the following steps to configure a route to the gatekeeper from LifeSize Transit Server through LifeSize Transit Client. Complete these steps before configuring video communications devices to use LifeSize Transit.

1. Ensure that LifeSize Transit Server and LifeSize Transit Client are installed on your network. Refer to ”Installation Requirements” on page 15.
2. Ensure that a user account for LifeSize Transit Client exists in the database on LifeSize Transit Server. Refer to ”Managing User Accounts” on page 18.
3. Configure the firewall to allow communication between LifeSize Transit Server and LifeSize Transit Client. Refer to ”Configuring Ports for LifeSize Transit” on page 22.
4. Access the LifeSize Transit Server web administration interface.
5. On the **Operation & Maintenance** menu, click **H.323 Configuration**.
6. For the **Gatekeeper mode**, ensure that **Use gatekeeper at private LAN** is selected. Click **Set** button at the bottom of the page.
7. Configure LifeSize Transit Client to communicate with LifeSize Transit Server:
   a. Access the LifeSize Transit Client web administration interface.
   b. On the **Operation & Maintenance** menu, click **Connection**.
   c. In the **User ID** section enter the user ID and password for LifeSize Transit Client. The username and password are the ones you entered in the **Tunnel** section of the **Create New User Account** page on LifeSize Transit Server when you created the user account for LifeSize Transit Client.
   d. Click the **Set** button to save the settings.
   e. In the **LifeSize Transit Servers** section, enter the IP address of the signaling server on LifeSize Transit Server in the **Servers** field.
   f. Click the **Set** button to save the setting.
   g. Ensure that the **Current Status** on this page changes to **Connected**.
8. For LifeSize Transit Server to be able to access the gatekeeper in the LAN through LifeSize Transit Client for incoming calls, add a route in LifeSize Transit Server to redirect incoming calls from the server to the gatekeeper in the private network through LifeSize Transit Client. Complete the following steps to add the route:
   a. Access the web administration interface of LifeSize Transit Server.

b. On the **Operation & Maintenance** menu, click **H.323 Routing**.

c. Enter a prefix in the **H.323 Prefix or Domain** field. Only alphanumeric characters, a period (.), and a hyphen (-) are allowed.

d. In the **H.323 Zone Gatekeeper host:port** field, enter the IP address of the gatekeeper in the private network.

e. In the **Tunnel via** field, enter the user ID of the LifeSize Transit Client. This is the user ID that you entered in the **Tunnel** section of the **Create New User Account** page when you created the user account for the LifeSize Transit Client.

f. In the **Vendor** list, select **Radvision** for the LifeSize Gatekeeper.

g. Click the **Add** button to add the route.

9. Configure the outbound prefix on LifeSize Transit Client for placing outbound calls:

   a. Access the web administration interface of LifeSize Transit Client.

   b. On the **Operation & Maintenance** menu, click **H.323 Settings**.

   c. If a connection between LifeSize Transit Client and LifeSize Transit Server was established successfully and the incoming route was added in step 8, the **Internal Gatekeeper Address** field is automatically populated with a value from the server. Ensure that the address of the gatekeeper is correct.

   d. In the **Outbound prefix at Gatekeeper** field, specify a prefix number for outbound calls. This must be a unique, numeric prefix not already in use by the gatekeeper and not the same as the prefix configured on LifeSize Transit Server for routing incoming call to the gatekeeper.

   e. Select the **Strip prefix from outbound calls** and **Register at Gatekeeper** check boxes.

   f. Click the **Set** button to save the settings.

   g. Ensure that the value of the **Registration status** field in the **Internal Gatekeeper Registration** section of this page is `Registered`.

      When LifeSize Transit Client registers with the gatekeeper, the registration automatically adds the outbound prefix as a user-defined service prefix in the gatekeeper. When the gatekeeper receives an outbound call that includes this prefix, it routes the call to LifeSize Transit Client. You can verify this setting on LifeSize Gatekeeper by accessing its web administration interface and navigating to the **Services** tab. The outbound prefix appears as a service prefix in the **Prefix** column.

Deploying LifeSize Transit Client with Built-In Gatekeeper

If you are using LifeSize Transit Client with the built-in gatekeeper in LifeSize Transit Server, complete the following steps before configuring video communications devices to use LifeSize Transit.

1. Ensure that LifeSize Transit Server and LifeSize Transit Client are installed on your network. Refer to ”Installation Requirements” on page 15.
2. Ensure that a user account for LifeSize Transit Client exists in the database on LifeSize Transit Server. Refer to ”Managing User Accounts” on page 18.
3. Configure the firewall to allow communication between LifeSize Transit Server and LifeSize Transit Client. Refer to ”Configuring Ports for LifeSize Transit” on page 22.
4. Access the LifeSize Transit Server web administration interface.
5. On the **Operation & Maintenance** menu, click **H.323 Configuration**.
6. For the **Gatekeeper mode**, ensure that **Use built-in gatekeeper** is selected.
7. Configure LifeSize Transit Client to communicate with LifeSize Transit Server:
   a. Access the LifeSize Transit Client web administration interface.
   b. On the **Operation & Maintenance** menu, click **Connection**.
   c. In the **User ID** section enter the user ID and password for LifeSize Transit Client. The username and password are the ones you entered in the **Tunnel** section of the **Create New User Account** page on LifeSize Transit Server. Click the **Set** button to save the settings.
   d. In the **LifeSize Transit Servers** section, enter the IP address of the signaling server on LifeSize Transit Server in the **Servers** field. Click the **Set** button to save the setting.
   e. Ensure that the **Current Status** on this page changes to **Connected**.
   f. On the **Operation & Maintenance** menu, click **H.323 Settings**.
   g. If you leave the **H460.18/19 Traversal Server** field empty, a tunneled connection will be used between LifeSize Transit Client and LifeSize Transit Server for H.323 communication. TCP port 444 will be tried first. If it is not available, TCP port 443 is used. If you wish to use the H.460.18/19 traversal server for this communication, enter the IP address of the signaling server in this field.

Configuring LifeSize Systems for Firewall Traversal

Before you configure LifeSize systems to work with LifeSize Transit, ensure that you have completed all preceding configuration instructions described in this guide that apply to the configuration option that you chose. Also ensure that the LifeSize systems that you wish to configure are installed with a software version that is compatible with the software version of LifeSize Transit that you are using. The software version of LifeSize Transit Server and LifeSize Transit Client appear on the home page of the web administration interface for these devices. The software version on LifeSize systems appears on the **System Information** page of the user interface and on the **Login** page of the web administration interface. Refer to the *LifeSize Transit Release Notes* at www.lifesize.com/support for a list of compatible software versions.

Configuring LifeSize Devices for SIP Firewall Traversal

If you are using LifeSize Transit for SIP firewall and NAT traversal, use the instructions in this section to configure Lifesize systems to use STUN, TURN, and ICE and the SIP registrar included with LifeSize Transit.

The configuration instructions differ depending on whether you are using LifeSize Transit Server alone or with LifeSize Transit Client. If you are using only LifeSize Transit Server complete the steps in ”Configuring LifeSize Devices for SIP with LifeSize Transit Server Only” on page 37. If you are using LifeSize Transit Client, complete the steps in “Configuring LifeSize Devices for SIP with LifeSize Transit Client” on page 40.

> ***Caution:*** Ensure that you configure preferences on your LifeSize systems in the order listed in this section. Otherwise, the LifeSize systems may register directly to the LifeSize Transit Server without using the SIP firewall traversal software included with the systems.

If you are not using SIP in your environment, skip this section and configure your LifeSize devices to use H.460 for H.323 calls. Refer to “Configuring LifeSize Devices for H.460 Firewall Traversal” on page 42.

Configuring LifeSize Devices for SIP with LifeSize Transit Server Only

1. Ensure that you have installed LifeSize Transit Server and created user accounts for each LifeSize system that you intend to use with LifeSize Transit. Refer to “Installation Requirements” on page 15 and “Managing User Accounts” on page 18.
2. Access the user or web administration interface of the LifeSize system that you wish to configure.

3. Configure the system to use SIP firewall traversal with LifeSize Transit Server by configuring the following preferences:

   a. Navigate to **Administrator Preferences : Network : LifeSize Transit**

   b. In the **Transit Hostname** field enter the IP address of the LifeSize Transit Server signaling server. This address appears on the home page of the LifeSize Transit Server web administration interface as the **Public Address** in the **Server Status** section of the page.

   c. In the **Transit Username** and **Transit Password** fields, enter the tunnel user ID and password that you created for the system in its user account on LifeSize Transit Server. Refer to ”Managing User Accounts” on page 18.

   d. Ensure that **Transit ICE** is set to *Enabled* (the default value).

   e. If you wish to use UDP SIP signalling when possible, choose *UDP,TCP* for the **Transit Signaling** preference. For the most reliable configuration, LifeSize recommends *TCP Only* (the default) as the setting for this preference.

   f. If your firewall only allows traffic through a web proxy, enter the web proxy address (URL), username, and password. Otherwise, leave these fields blank.

   g. Choose *Enabled* for the **LifeSize Transit** preference to use LifeSize Transit to manage calls.

   h. Ensure that the LifeSize Transit Status that appears on this page is **Connected**.

   Caution: Enabling LifeSize Transit in automatically configures the **SIP Proxy**, **Proxy Hostname**, and **Proxy IP Port** preferences in **Administrator Preferences : Communications : SIP**. Do not change these settings.

4. Configure the LifeSize system to use the LifeSize Transit SIP registrar by configuring the following preferences:

   a. Navigate to **Administrator Preferences : Communications : SIP**.

   b. Ensure that the **SIP** preference is set to *Enabled*.

   c. For the **SIP Username** and **Authorization Name** preferences, enter the **SIP Digest User Name** that you entered in the user account for this system in LifeSize Transit Server. Refer to “Creating User Accounts” on page 19.

   d. For the **Authorization Password** preference, enter the **Password** that you entered in the **SIP and H.323** section of the **Create New User Account** page when you created a user account for this system in LifeSize Transit Server. Refer to “Creating User Accounts” on page 19.

e. Ensure that **SIP Server Type** is set to *Auto*.

f. Ensure that **SIP Registration** is set to *Through Proxy*.

Caution: Enabling LifeSize Transit in step 3 automatically configures the **SIP Proxy**, **Proxy Hostname**, and **Proxy IP Port** preferences. Do not change these settings.

g. Choose *Enabled* for the **SIP Registrar** preference.

h. For the **Registrar Hostname** preference, enter the SIP domain on the LifeSize Transit server (which might be its IP address).

i. For the **Registrar IP Port** preference, enter the IP port number of the SIP registrar server. The default port is 5060.

j. Accept the defaults for the UDP Signaling Port (5060), TCP Signaling (Disabled), and TLS Signaling (Disabled).

k. Select the **Register** button and press **OK**. The **Registrar Status** above the **Register** button changes to **Registered** if the registration is successful.

5. You can test the configuration by completing the following steps:

a. Access the web administration interface of LifeSize Transit Server.

b. On the **Operation & Maintenance** menu, click **Connected Clients**.

c. Ensure that the SIP registration for the system appears on this page.

d. Place a call from the system to a another SIP video communications system that has a public IP address by dialing the sip*:IP address* of the SIP user you are calling.

e. On the **Operation & Maintenance** menu of LifeSize Transit Server, click **Call Status**.

f. Ensure that the call appears in the **Active Calls** section.

g. Place a SIP call from a system that has a public IP address, if available, to this system by dialing *sip_user@signaling_IP* where *sip_user* is the SIP user name of the system and *signaling_IP* is the IP address of the LifeSize Transit signaling server. Repeat steps e and f for this call.

Configuring LifeSize Devices for SIP with LifeSize Transit Client

1. Ensure that you have installed LifeSize Transit Server and LifeSize Transit Client and created user accounts for each LifeSize system that you intend to use with the product and a user account for LifeSize Transit Client. Refer to “Installation Requirements” on page 15 and “Managing User Accounts” on page 18.
2. Access the administrative or web administration interface of the LifeSize system that you wish to configure.
3. Configure the LifeSize system to use the LifeSize Transit Client as the SIP proxy and the LifeSize Transit Server as the SIP registrar by configuring the following preferences:
   a. Navigate to **Administrator Preferences : Communications : SIP**.
   b. Ensure that the **SIP** preference is set to *Enabled*.
   c. For the **SIP Username** and **Authorization Name** preferences, enter the **SIP Digest User Name** that you entered in the user account for this system in LifeSize Transit Server. Refer to “Creating User Accounts” on page 19.
   d. For the **Authorization Password** preference, enter the **Password** that you entered in the **SIP and H.323** section of the **Create New User Account** page when you created a user account for this system in LifeSize Transit Server. Refer to “Creating User Accounts” on page 19.
   e. Ensure that **SIP Server Type** is set to *Auto*.
   f. Ensure that **SIP Registration** is set to *Through Proxy*.
   g. For the **SIP proxy** preference, choose *Enabled*.
   h. In the **Proxy Hostname** preference, enter the IP address of the LifeSize Transit Client.
   i. Ensure that the **Proxy IP Port** is set to *5060*.
   j. For the **SIP Registrar** preference, choose *Enabled*.
   k. In the **Registrar Hostname** preference, enter the SIP domain on the LifeSize Transit server (which might be its IP address).
   l. Ensure that **Registrar IP Port** is set to *5060*.
   m. Accept the defaults for the UDP Signaling Port (5060), TCP Signaling (Disabled), and TLS Signaling (Disabled).
   n. Select the **Register** button and press **OK**. The **Registrar Status** above the **Register** button changes to **Registered** if the registration is successful.

4. You can test the configuration by completing the following steps:
   a. Access the web administration interface of LifeSize Transit Server.
   b. On the **Operation & Maintenance** menu, click **Connected Clients**.
   c. Ensure that the SIP registration for the system appears on this page.
   d. Access the web administration interface of LifeSize Transit Client.
   e. On the **Operation & Maintenance** menu, click **Registered Users**.
   f. Ensure that the SIP registration for the system appears on this page.
   g. Place an outbound call from the system to another video communications system that has a public IP address by dialing sip*:IP_address* of the SIP user you are calling
   h. On the **Operation & Maintenance** menu of LifeSize Transit Server, click **Call Status**.
   i. Ensure that the call appears in the **Active Calls** section.
   j. On the **Operation & Maintenance** menu of LifeSize Transit Client, click current calls
   k. Ensure that the call appears in the **Current Calls** section.
   l. Place an inbound call from a system that has a public IP address, if available, to this system by dialing *sip_user@signaling_IP* where *sip_user* is the SIP user name of the system you are calling and *signaling_IP* is the IP address of the LifeSize Transit signaling server. Repeat steps h through k for this call.

Configuring an MCU for SIP with LifeSize Transit Client

The following configuration instructions are specifically for a Codian MCU but an analogous procedure applies to LifeSize Multipoint MCUs. Use the Transit Server IP address as the SIP registrar domain and use the Transit Client IP address as the SIP proxy address.

1. Ensure that you have installed LifeSize Transit Server and LifeSize Transit Client and created user accounts for each Codian MCU that you intend to use with the product and a user account for LifeSize Transit Client. Refer to “Installation Requirements” on page 15 and “Managing User Accounts” on page 18.
2. Access the administrative or web administration interface of the Codian MCU that you wish to configure.

3. Configure the Codian MCU to use the LifeSize Transit Client as the SIP proxy and the LifeSize Transit Server as the SIP registrar in the SIP settings page by completing the following steps:
   a. Select **Allow conference registration** for **SIP registration settings**.
   b. For **SIP registrar domain**, enter the Transit Server IP address.
   c. Select **Standard SIP** for **SIP registrar type**.
   d. Enter the username and password you created for the MCU in step 1.
   e. For **SIP proxy address**, enter the Transit Client IP address.

Configuring LifeSize Devices for H.460 Firewall Traversal

LifeSize systems support the H.460 protocol for firewall and NAT traversal of H.323 calls. By default, H.460 is disabled on LifeSize systems. If you are using LifeSize Transit for H.323 calls, use the instructions in this section to configure LifeSize systems for firewall traversal of H.323 calls with LifeSize Transit. The configuration instructions differ depending on whether you are using LifeSize Transit Server alone or with LifeSize Transit Client.

If you are using only LifeSize Transit Server complete the steps in “Configuring LifeSize Devices for H.460 with LifeSize Transit Server Only” on page 42. If you are using LifeSize Transit Client with a private gatekeeper in the LAN, complete the steps in ”Configuring LifeSize Devices for H.323 with LifeSize Transit Client and a Private Gatekeeper” on page 43. If you are using LifeSize Transit Client with the built-in gatekeeper of LifeSize Transit Server, complete the steps in ”Configuring LifeSize Devices for H.323 with LifeSize Transit Client and Built-In Gatekeeper” on page 44

Configuring LifeSize Devices for H.460 with LifeSize Transit Server Only

1. Ensure that you have installed LifeSize Transit Server. Refer to “Installation Requirements” on page 15.
2. Access the user or web administration interface of the LifeSize system that you wish to configure.
3. Navigate to **Administrator Preferences : Communications : H.323**.
4. Configure the preferences on this page as described in the *LifeSize Video Communications Systems Administrator Guide* in the section “Specifying H.323 Settings” with the following exceptions:
   a. Choose *Manual* for the **Gatekeeper Mode** preference.
   b. For the **Gatekeeper IP Address 1**, enter the IP address and port number of the LifeSize Transit signaling server.

c. Ensure that the **Gatekeeper Port 1** preference is set to *1719* (the default).

d. Choose *Enabled* for the **H.460** preference.

e. Navigate to **Register** and press **OK**.

Note: If you enable H.460 and specify the IP address and port number of a secondary gatekeeper with the **Gatekeeper IP Address 2** and **Gatekeeper Port 2** preferences, the system ignores the secondary gatekeeper. The system also ignores preferences in **Administrator Preferences : Network : NAT**. The gatekeeper user name and password fields are not supported.

5. Test the configuration by completing the following steps:

   a. Access the web administration interface of LifeSize Transit Server.

   b. On the **Operation & Maintenance** menu, click **Connected Clients**.

   c. Ensure that two registration entries appear for the system: one for H.323 and one for the H.323 extension.

   d. Place an outbound call from the system to another video communications system that has a public IP address by dialing the public IP address.

   e. On the **Operation & Maintenance** menu of LifeSize Transit Server, click **Call Status**.

   f. Ensure that the call appears in the **Active Calls** section.

   g. Place an inbound call from a system that has a public IP address, if available, to the system by dialing *<signaling_server_IP>##<H.323_Extension>* where *<signaling_server_IP>* is the IP address of the LifeSize Transit signaling server and *<H.323_Extension>* is the H.323 Extension of the system you are calling.

   h. Repeat steps e and f.

Configuring LifeSize Devices for H.323 with LifeSize Transit Client and a Private Gatekeeper

1. Ensure that you have completed the configuration steps in “Deploying LifeSize Transit Client with a Private Gatekeeper” on page 34.

2. On each LifeSize video communications system that you intend to use with LifeSize Transit, access either the web administration interface or the user interface and navigate to **Administrator Preferences : Communications : H.323**.

3. Configure the preferences on this page as described in the LifeSize Video Communications Systems Administrator Guide in the section “Specifying H.323 Settings” with the following exceptions:

   a. Add the route prefix that you created in LifeSize Transit Server (the **H.323 Prefix or Domain** field) to the beginning of the value in the **H.323 Extension** preference. For example, if the route prefix is 22 and the H.323 extension of the video communications system is 1234, then the value of the H.323 Extension preference is 221234.

   b. Choose *Manual* for the **Gatekeeper Mode** preference.

   c. For the **Gatekeeper IP Address 1** and **Gatekeeper Port 1** preferences, enter the address of the gatekeeper in the private LAN.

   d. Ensure that **H.460** is set to Disabled (the default).

   Note: If you enable H.460 and specify the IP address and port number of a secondary gatekeeper with the **Gatekeeper IP Address 2** and **Gatekeeper Port 2** preferences, the system ignores the secondary gatekeeper. The system also ignores preferences in **Administrator Preferences : Network : NAT**. The gatekeeper user name and password fields are not supported.

4. Navigate to Register and press OK.

5. Test the configuration by placing an outbound call. The device can call another device with a public IP address that is not registered to the internal gatekeeper using the dial string <outbound_prefix>##<public_IP_address> or <outbound_prefix><public_IP_address>. Both dialing patterns are supported.

Configuring LifeSize Devices for H.323 with LifeSize Transit Client and Built-In Gatekeeper

1. Ensure that you have completed all steps in “Deploying LifeSize Transit Client with Built-In Gatekeeper” on page 36.

2. Access the user or web administration interface of the LifeSize system that you wish to configure.

3. Navigate to **Administrator Preferences : Communications : H.323**.

4. Configure the preferences on this page as described in the *LifeSize Video Communications Systems Administrator Guide* in the section “Specifying H.323 Settings” with the following exceptions:

   a. Choose *Manual* for the **Gatekeeper Mode** preference.

b. For the **Gatekeeper IP Address 1** preference, enter the IP address of LifeSize Transit Client.

c. For the **Gatekeeper Port 1** preference, ensure that it is set to *1719* (the default).

d. Ensure that the **H.460** preference is set to *Disabled* (the default).

5. Navigate to **Register** and press **OK**.

6. Test the configuration by completing the following steps:

   a. Access the web administration interface of LifeSize Transit Server.

   b. On the **Operation & Maintenance** menu, click **Connected Clients**.

   c. Ensure that the H.323 registration for the system appears on this page and that `H.460.18` appears in the **Transport** column.

   d. Access the web administration interface of LifeSize Transit Client.

   e. On the **Operation & Maintenance** menu, click **Registered Users**.

   f. Ensure that the H.323 registration for the system appears on this page and `H.460` appears in the **Mode** column.

   g. Place an outbound call from the system to another video conference system that has a public IP address by dialing the IP address.

   h. On the **Operation & Maintenance** menu of LifeSize Transit Server, click **Call Status**.

   i. Ensure that the call appears in the **Active Calls** section and `H.460` appears in the **Transport** column.

   j. On the **Operation & Maintenance** menu of LifeSize Transit Client, click current calls.

   k. Ensure that the call appears in the **Current Calls** section and `H.460_client` appears in the **MediaMethod** column.

   l. Place an inbound call to the system from a video conference system with a public IP address by dialing *<signaling_server_IP>##<H.323_Extension>* where *<signaling_server_IP>* is the IP address of the LifeSize Transit signaling server and *<H.323_Extension>* is the H.323 Extension of the system you are calling.

   m. Repeat steps h through k.

Configuring an MCU for H.323 with LifeSize Transit Client

If you are using a standalone gatekeeper in the private LAN, you do not need to change your MCU settings. If there is no standalone gatekeeper, specify the Transit Client IP address as the gatekeeper IP in the MCU's administration interface.

Configuring LifeSize Desktop for use with LifeSize Transit

If you are using LifeSize Desktop to place calls to other LifeSize devices or LifeSize Desktop installations in your organization through LifeSize Transit, you must configure LifeSize Desktop to use LifeSize Transit. For configuration instructions, refer to the technical note *Configuring LifeSize Desktop for Use with LifeSize Transit*. This technical note is available at lifesize.com/support.

Database Backup and Restore

To back up the server database, follow these steps:

1. Access the web administration interface of LifeSize Transit Server. Refer to "Accessing the Web Administration Interface" on page 16.
2. Click **Additional Maintenance Tasks** on the menu. If you are prompted for a username and password, enter the LifeSize Transit username and password.
3. From the **LifeSize Transit Server Utilities** page, click **Database Backup**.
4. Click **Start Backup**.
5. Click **Download** to save the backup file to a local directory.

To restore the server database, follow these steps:

1. Follow the previous procedure to back up the server database.
2. From the **LifeSize Transit Server Utilities** page, click **Database Restore**.
3. Enter or browse for the database backup file you created in the previous procedure.
4. Click **Start Restore**.

Upgrading Software

Before upgrading LifeSize Transit software, note the serial number of the device that you wish to upgrade. The serial number is visible in the web administration interface. Refer to ”Accessing the Web Administration Interface” on page 16. For LifeSize Transit Server, navigate to the **Additional Maintenance Tasks** page and then click **Version Information**. For LifeSize Transit Client, navigate to the **Configuration** page.

> ***Caution:*** An upgrade ends calls in progress. LifeSize recommends that you upgrade LifeSize Transit during off peak hours of use. Navigate to the **Call Status** page in the web administration interface of LifeSize Transit Server or the **Current Calls** page in the web administration interface of LifeSize Transit Client and ensure that no calls are connected before performing the upgrade. Refer to “Call Status Page” on page 48 for LifeSize Transit Server and “Current Calls” on page 72 for LifeSize Transit Client.

Follow these steps to upgrade the software for LifeSize Transit:

1. Obtain the upgrade software package from the Support page of lifesize.com/support. Click the **Download Software** link and follow the instructions that appear.
2. Access the web administration interface of the device you wish to upgrade.
3. On the **Operation & Maintenance** menu, click **Software Upgrade**.
4. Browse for the upgrade file that you downloaded in step 1.
5. Click **Start Upgrade**.

   Note: This may take several minutes; do not disrupt the upgrade process.

   A system upgrade status message appears when the upgrade is complete.

Troubleshooting

This section describes the most common issues that you may encounter with a LifeSize Transit deployment.

Invalid DNS Configuration

LifeSize Transit Server fails to function properly if it is not configured to use a valid, available DNS server. Ensure that you have properly configured the DNS settings on the server and that the DNS server is available.

Server Connections

If the media server is not connected, as indicated on the **Home** or **Media Engine Configuration** pages in the LifeSize Transit Server web administration interface, click the **Restart** button in the **Media Engines** section on the **Media Engine Configuration** page or in the **Perform Tasks** section for the media engines in the **Server Configuration** page.

Rebooting LifeSize Transit

You can reboot LifeSize Transit Server from its web administration interface. On the **Operation & Maintenance** menu, click **Additional Maintenance Tasks**. When prompted for login credentials, enter the username and password for the web administration interface. On the **LifeSize Transit Server Utilities** page that appears, click Reboot Transit Server.

Call Status Page

The **Call Status** page of the LifeSize Transit Server web administration interface lists up to 20 active calls and 20 closed calls. Failed calls appear in red in the **Closed Calls** table. Use the **Filter string** text box and **Submit Query** button in the **Closed Calls** section to search for additional closed calls. Use the **End reason** field in the details of each call to troubleshoot a failed call.

Field	Description
Maximum relayed calls	The maximum number of relayed calls permitted.
Active calls	Originating Side of Call: # is a linked image. Click the image to view additional details about the call. ***User ID*** is the SIP/H.323 ID of the originating user. ***RealTunnel ID*** is the LifeSize Transit user ID of the originating user. ***Public Address*** is the public IP address of the originating user. Terminating Side of Call: ***User ID*** is the SIP/H.323 ID of the terminating user. ***RealTunnel ID*** is the LifeSize Transit user ID of the terminating user. ***Public Address*** is the public IP address of the terminating user. Common Info: ***Start time*** is the date and time this call was started. ***Duration (sec)*** is the duration of the call in seconds. ***Protocol*** is the protocol being used in the call.
Closed Calls	The fields are identical to the Active Calls fields. The data that appears is for calls that are no longer active.

You can view the following details about a call for the calling and called parties by clicking the arrow at the left of each call row:

Field	Description
Call Identifier	Unique call identifier for the call that is useful when matching records from multiple systems.
Public address	Public address of the endpoint. It may also be the address of a remote SIP server/gatekeeper if it hides the internal addresses.
Country	Location of the caller/callee.
Private address	Actual IP address the calling/called device is given. This may also be the address of a remote SIP server/gatekeeper.
Client type	Device identifier as reported by the device. This may be blank if not reported by the device.
Client version	LifeSize Transit client version if the caller/callee utilizes this.
End reason	This is reported in closed calls. Refer to “Error Messages” on page 50 for a list of reasons a call may fail.
Transport	Traversal method used for this media stream.
Allocated address	Media address and port for the media stream as presented to the remote video communications system. Can be a host address, server relayed address, or discovered address.
Remote address	Remote address to which this side sends media.
Down kB	Bandwidth so far received by the caller/callee for this stream (updated every 60 seconds).
Up kB	Bandwidth so far sent by the caller/callee for this stream (updated every 60 seconds).

Error Messages

The following messages may display on the **Call Status** page in the **End reason** field of the details for a call.

Message	Description
UNKNOWN	Unknown reason.
NORMAL	The call terminated normally.
USER_UNREG	The user unregistered during a call.
USER_FORCED_UNREG	The user was forced to unregister (signed in from another location, or unregistered by the operator).
PXC_CONN_LOST	The signaling connection to the client was lost.
MESSAGE_IN_BAD_STATE	Received a disrupted message.
RESERVE_MEDIA_FAILED	Failed reserving media. Most often seen if the signaling server is not connected to the media engine. Refer to the home page or the Media Engine Configuration page in the web administration interface of the LifeSize Transit Server to view the connection status of the media engine.
JOIN_MEDIA_FAILED	Failed joining media. Most often seen if the signaling server is not connected to the media engine.
IO_FAIL_SENDING_MSG	An input or output failure occurred when attempting to send a message.
NO_RESPONSE_TO_INVITE	Did not receive a response to the invite.
INVITE_REJECTED	The invite was rejected.
ME_TUN_CONN_FAIL	Tunnel connection failed towards the media engine.
NO_RESPONSE_TO_OK	A SIP participant in a call did not receive confirmation that a participant to whom it sent a final messagehad received the message.

Message	Description
BAD_SDP	Trouble decoding the SDP in the SIP message, or the media type is unsupported.
FORCED_DOWN_UNREGD	Call forced down due to an unregistered user.
TUNNEL_DOWN	Signaling connection lost during media transfer.
CONN_FAILED_IN_PXS	Failed to connect two users in PXS.
CALL_ENDED_BY_ME	The call was ended by the media engine (most likely if it detected a lost TCP connection from the client).
PXS_LOST_CONN_TO_ME	The PXS lost its connection to the media engine.
CALL_REL_TIMEOUT	The call was released due a timeout.
BAD_SIP_MESSAGE	The recipient SIP user could not interpret the request.
SIP_AUTHENTICATION_FAILURE	A SIP server required authentication, but authentication data was missing or invalid authentication data was sent.
SIP_USER_NOT_FOUND	The (external) user was not found.
EXTERNAL_SERVER_UNAVAILABLE	The external server was temporary unavailable.
USER_BUSY	The user is busy and cannot accept more calls.
EXTERNAL_TIMEOUT	A request to an external server timed out.
USER_REJECTED	The user declined the call.
HANGING_CALL	Bandwidth usage is null over a long time.
CLIENT_CONNECTION_LOST	The signaling connection to the client was lost (from the server).
USER_TEMPORARY_UNAVAILABLE	The user was temporary unavailable or is not logged on.

Message	Description
NOT_END_TO_END_MEDIA	Signaling was okay, but media end-to-end did not occur both ways.
INCOMPATIBLE_MEDIA	A single compatible codec in SDP was not located.
OAM_CLOSED	The call was forced down by the operator.
ME_LOST_CONN_TO_CLIENT	The media engine lost connection to the client.
ME_TUN_CONN_LOST	Connection to the media engine was lost.
FAILED_TO_CONN_USERS	Failed to connect to the users.
MEDIA_FAILED_SIP_OK	Failed to create a connection to the media engine (but the INVITE was accepted).
CALLER_CANCELLED	The caller cancelled the call before anyone answered (most likely the called party did not answer).
MAX_CALL_CAP_REACHED	The maximum call capacity in the PXS has been reached.
SOCKET_FAILURE	The call failed due a local socket/network failure.

Event Reporting

The **Event Reporting** page in the web administration interface of LifeSize Transit Server enables you to configure and display the event status of the signalling server.

Field	Description
Mail Configuration	Enables you to configure where mail is sent when events are registered in the signalling server. **Outgoing SMTP server** is the outgoing SMTP server address. **Mail username** is the username to use to authenticate at the SMTP server. **Mail password** is the password to use to authenticate at the SMTP server. **Mail recipients** is mail addresses of the recipients separated by a comma.

Field	Description
Trap Receiver	Configures where traps are sent when events are registered in the signaling server. **Trap receiver address** is the address of the trap receiver.
Event Table	Shows the history of events on this server. **Event table size** is the maximum number of events stored in the table. The event table shows the following columns: # is the event number. **Event Name** is the logical name of the event. **Severity** is the severity of the event (corresponds to log level for each event). Color coding denotes the severity of the event. Red denotes severe. Yellow denotes warning. Green denotes information. Light green denotes the least severity.Refer to ”Logging” on page 68. **Info** is a textual explanation of the event. **Raised** is the timestamp when the event was raised. **Cleared** is the timestamp when the event was cleared. **Customer ID** is the ID of the customer. **Key** is a unique ID of the event. **Local Address** is the address of the host of the event. **Action** defines possible actions to handle the event.

Diagnostic Files and Utilities

The following features assist you in troubleshooting issues that you may encounter with LifeSize Transit. Use these features only if directed to do so by a LifeSize Technical Services representative.

Log Files

When abnormal behavior has been detected in any of the LifeSize Transit clients, the signaling server or the media server, information about this behavior may appear in the log files. Refer to ”Logging” on page 68 for information about how to download log files. LifeSize Technical Services may instruct you to download and send these files to LifeSize for analysis if needed.

Capturing Diagnostic Information

You can download a file that contains diagnostic information from the **Diagnostics** page on the LifeSize Transit Client web administration interface and from the **Diagnostics file** on the **Additional Maintenance Tasks** page of the LifeSize Transit Server web administration interface. Create this file only when instructed to do so by a LifeSize Technical Services representative.

Enabling Remote Diagnostic Access

The **Remote Diagnostic Access** fields on the LifeSize Transit Client **Diagnostics** page enables remote access to your installation for troubleshooting purposes with a LifeSize Technical Services representative. Refer to your LifeSize Technical Services representative for instructions.

Downloading Call Detail Records

You can also download call detail records (CDRs) from the **Additional Maintenance Tasks** page of the LifeSize Transit Server web administration interface by clicking **Call Detail Records** and then clicking **CDR File Download**. This is a text file that contains information available in the **Closed Calls** section of the **Call Status** page.

Appendix A: LifeSize Transit Server Configuration Settings

Several LifeSize Transit configuration settings are preconfigured in the **Operation & Maintenance** user interface. Unless specifically instructed in the deployment scenarios described in this guide or by a LifeSize Technical Services representative, LifeSize recommends that you do not change them. The following tables describe these settings for LifeSize Transit Server and are for reference only. Consult LifeSize Technical Services if you need assistance modifying your configuration. Refer to ”Appendix B: LifeSize Transit Client Configuration Settings” on page 70 for information about configuration settings for LifeSize Transit Client.

Home Page

The home page displays a menu of operation and maintenance functions, as well as links to provisioning from which you can list, search, and create users. The status of events and the server appear and include the following data:

Label	Description
Event Status	An overview of the most important events reported by the server. Events marked “Severe” and “Warning” may indicate a serious problem with the server. Click any of the event icons, event levels, or **Show event table** to open the Event Reporting page. Refer to ”Event Reporting” on page 52.
Server Status	
Proxy Server Version	The version of the signalling server.
Media Engine Version	The version of the media server.
Public Address	The public address of the signalling server.
Current Time	The system time of the machine on which the signalling server is running.
Running Time	The length of time the server has been running since the last restart (hours:minutes:seconds).
Startup Time	The time at which the signalling server was started.
Media Engines	Indicates if the defined media engines are connected.
Connected Clients	The status of the connected (tunnelled) clients.

Label	Description
Local Current Calls	The status of the current calls in the Signalling Server (for example, total, failed, average call time, bandwidth usage, etc.)
Public SSL Certificate expiry date	Indicates when the public SSL certificate expires.
License Expire Date	Indicates when the license for the signalling-server will expire.
Home	Indicates the current software version of LifeSize Transit Server.

Connected Clients

An H.323 device can register both an H.323 ID and H.323 Name and each will be listed here. MCUs can have multiple User IDs and each will be listed here.

Click **Connected Clients** to display all connected clients with the following information..

Label	Description
User ID/Domain	The SIP/H.323 user ID the user is logged into as the SIP/H.323 client. If this is a domain registration, the registered domain appears instead.
RealTunnel ID	The internal RealTunnel user ID. This only appears for SIP or H.460 registrations through a Transit Client.
Version	The software version ID of the client.
Domain	A check mark appears in this field if this entry is a domain registration.
Private Address	The private IP address of the connected client.
Protocol	The protocol used when registering the video communications device, typically SIP or H.323.
Transport	The transport protocol used when connecting the video communications device. Possible values include Tunnel-TCP; Tunnel-HTTPS; H.460 for H.323 devices; or UDP or TCP SIP registrations.
Public Address	The public address of LifeSize Transit Client if used.
Proxy Address	The address of the HTTP(S) proxy, if used.

Label	Description
Proxy Auth	The authentication scheme used in the HTTP proxy.
NAT	The NAT type of the LAN where LifeSize Transit Client is running.
Type	The type of SIP/H.323 client which is a free string provided by the video communications device.
Duration	Indicates how long LifeSize Transit Client has been connected.

Server Configuration

The **Server Configuration** page identifies basic system parameters for the signalling server.

Label	Description
Perform Tasks	
Restart signalling server and Restart all media servers	Restarts the specified servers. Restart immediately terminates all calls and client connections.
Manage SSL/TLS certificate	Takes you to the certificate management page where you can manage the server's SSL certificate.
Proxy Server Address and Ports	
Signaling server public address	Reserved for future use.
Enable SSL tunneling ports	Enable or disable port 443 (standard HTTPS). The default is enabled (selected).
Enforce encrypted SSL	Sets the server to only accept encrypted SSL connections. LifeSize systems will not be enabled to connect with the default configuration when this is enabled. They must be manually configured to connect using the encrypted SSL. LifeSize recommends that you do not enable this feature.
Enable TCP tunnel port	Enable or disable port 444. The default is enabled (selected).

Database Configuration

The **Database Configuration** page contains configuration settings for authenticating user transactions and for configuring the connection to the database.

The following types of transactions are authenticated:

- tunnel connections
- SIP transactions (by the registrar)
- TURN allocations

Note: The same authentication method must be used for all of these transactions.

Option	Description
Database Mode	No database: If local authentication is set and the registrar functionality is disabled, disable the database. Connect directly to database: You use the database to authenticate LifeSize Transit users and provide SIP authentication. This is the default setting and is already completely configured. **LifeSize recommends you do not change this setting.** Use Master Signalling Server as Database: Reserved for future use.
Set time of day to run database vacuuming:	You can specify the hour at which to run database vacuuming. Database vacuuming is necessary if you use PostgreSQL as your database. Vacuuming cleans and optimizes database access once a day. The time at which vacuuming occurs is configurable. Enter a value from 0 to 23 (0 equal to midnight and 12 equal to noon). The default is 4. Click **Set**.
Database Settings	Database connection status shows whether the database is connected or not (with a description of why if not connected). **Database URL**, **User** and **Password** are properties needed when connecting to the database.
Authentication Settings	
Authentication mode	To authenticate tunnel connections, SIP registrations and TURN relay traffic, four modes are supported: **Fixed**: The same password is used for all users. **Database**: Each user has its provisioned entry in the database with a give password (the default). **RADIUS**: Reserved for future use. **Plugin**: A tailored authentication module can be used. Contact LifeSize if you need to implement a different authentication mechanism.

Option	Description
Allow multiple tunnelled clients using the same ID	The default is **Do not allow**. If set to **Allow**, the **Password for Fixed Authentication** field is available for specifying the password.

Media Engine Configuration

The **Media Engine Configuration** page shows the media engine connection status.

Field	Description
Multi TCP Configuration	Multi TCP is a way to optimize media traffic over TCP by using more than one TCP connection per media stream. It generally improves the media quality in congested networks, but can also cause the RTP packets to be received out of order. It works best with clients with good sequence control and jitter buffers for received media packets. Enable multi-TCP on audio: Enables/disables multi-TCP on audio. The default is enabled (selected). Enable multi-TCP on video: Enables/disables multi-TCP on video. The default is disabled (not selected).
Media Configuration	**Enable application sharing in PXS**: Enables/disables application sharing. **Allow direct media between clients**: Enables/disables direct media between clients configured for LifeSize Transit. **Monitor media flow every**: You can specify the number of minutes after which inactive media streams are closed or specify -5 or 0 to disable this feature. The default is 60 minutes.

Field	Description
Media Relay	
Enable UDP relay for non-tunneling clients behind NAT	The signalling server can relay RTP/UDP media for SIP clients without LifeSize Transit clients. For users behind relaxed NAT devices (allowing UDP traffic out) this is an attractive option as the LifeSize Transit client is not needed. You can control the level of media relay as follows: **All**: All calls routed through the signalling server are relayed, regardless of whether they need it or not. This leads to excessive relaying and is not recommended. **Non-Ice**: Relaying media for all calls placed without using ICE. **All NAT**: Relaying media for all users in need, when either the calling or called client is behind NAT (and do not support STUN). This is the default selection. **Local Users**: Behaves the same as All NAT, except relay only occurs for the authenticated users local to this registrar. **None**: Disables UDP relay. This setting does not affect the behavior of calls to or from a tunnelling client.
Use of direct media based on public address	While inducing relay for NATed clients helps for NAT traversal, it comes with a cost of increased bandwidth usage. LifeSize Transit can judge if the two clients in a call are on the same LAN, based on their public IP address. This field allows configuration of an exclusion pattern following the media relay level previously described in this table. In cases with complex or nested NATs this exclusion can lead to media failures, but it makes sense to enable this on an enterprise deployment, if you know there is only one NAT device on the local network. Note that this exclusion pattern also applies to H.460 traversal. H.460 calls between clients judged to be on the same LAN below will not have media relayed through the LifeSize Transit Server. **No override**: Do not use the public IP address to avoid media relay. This is the default selection. **Use direct media for UDP registration behind the same public address**: Avoid media relay when the two clients in a call are behind the same IP address. **Use custom mapping of public addresses to LANs**: Allows a more flexible definition of which IP addresses are the public front of a LAN. If you need to specify individual addresses or address ranges that do not fit in a single IP/mask specification, use multiple lines mapping to the same nickname. If there are overlapping entries in the table, the longest prefix match is selected. If no mask is specified, a 32-bit mask (single address) is used. When you enable this option, the **Public to Same LAN mapping** table appears. You can add a new mapping by entering the public IP address and corresponding LAN nickname and clicking the **Add** button.

Field	Description
Media Engines	The **Connected** column for the media server shows the value **Yes** to indicate that the media server is connected.

STUN Server Configuration

LifeSize Transit Server includes both a STUN (RFC 3489) server and a STUN Relay (previously known as TURN) server, both available to the LifeSize Transit clients and external clients. The ports should be reachable through a DNS SRV query with the service “stun” and “turn”. Refer to ”Configuring DNS SRV Records for SIP” on page 17. Any firewalls in front of the server should open these ports as well. Refer to ”Configuring Ports for LifeSize Transit” on page 22. Changing any of the ports on this page requires a restart before a new value takes effect.

Field	Description
STUN Server ports	Displays the UDP ports used for the STUN servers. A STUN server requires two ports on the primary server, plus a third port on another IP address for checking the network connection. The signaling server is always the primary STUN server, while the primary media server is used as the secondary STUN server. The recommended port is 3478, but since older LifeSize Transit clients use the port 34501 use this as the secondary STUN port for backwards compatibility. The port set in **Port One** corresponds to the port returned by the DNS queries.
Remote STUN Server Ports	Sets the STUN port on the media server, and should correspond to what is set in its configuration file. The default is 34501 if not set.
TURN Server	These settings control the behavior of the TURN server. This is an independent protocol which non-LifeSize Transit clients can use as well. TURN requests require authentication, with the same user ID and password as used with LifeSize Transit clients. The signaling server authenticates these, and allows the media server do the actual relaying of media, so the clients need to support redirections of the TURN requests. **Enable TURN Server**: If selected (the default), the TURN server is enabled. **TURN Port**: The server port (UDP/TCP) for TURN used on the signaling server. The default is 3560. **TURN Port on the media server**: The server port for TURN used on the media server. The default is 3560. **Enable redirect based on TURN client location**: Like the tunnelling connections, the TURN clients can be directed to the TURN server closest to them, to reduce the latency and give better media quality in a call.

SIP Configuration

You can configure various SIP parameters from the **SIP Configuration** page.

Field	Description
SIP ports	LifeSize recommends you do not change this parameter. If you alter the value of this port, you must modify all clients (not recommended) and restart the server. Use the standard SIP port 5060.
UDP packet size	The server can receive and send SIP requests over TCP. If UDP messages are larger than the maximum transmission unit (MTU), they are fragmented and there is a risk they will not be received correctly by all hosts. To avoid UDP fragmentation, outbound requests are sent over TCP if they exceed a certain size. This size is 200 bytes less than the known MTU, or 1300 bytes if the MTU is unknown. Note that if a particular transport is enforced in the routing table on the SIP Routing page, this setting will not take effect.
Incoming Redirect Messages	Controls how the server acts on incoming redirect (3xx) messages. For example, a redirect server can send a 302 Moved Temporarily message in response to an INVITE, with the address of the client. The default behavior is enabled which sends the INVITE again to the new locations. If disabled, this redirect message is sent upstream to the calling client which can again perform the redirection.
Home Routing	If selected (the default), the signalling server routes requests from non-local users to their home proxy rather than to the destination. This preserves home based services and authentication and has no effect for users who are local on this server (the registrar is enabled).
Domain Registration Policy	The server provides resources (processor power and bandwidth) to users. You can restrict this usage to certain groups by creating a set of SIP domains users are allowed to log on to through this server; registrations of all other domains are rejected. Local users (if the registrar is enabled) will always be allowed regardless of this setting. Local users can still place and receive calls from other domains. If left empty, registrations are allowed for all domains.

SIP Registrar Settings

You can configure the following parameters for the signalling server on the **SIP Registrar Settings** page..

Field	Description
SIP domains	SIP domains are local; LifeSize Transit searches for these domain names in the database. For these domains to be callable from other systems, add these domain names to the DNS for this host.

Security Level	**Full**: All requests are authenticated. **Medium**: All requests are authenticated, except from the tunneled clients connected to this proxy server, where only REGISTER is authenticated. This is the default selection. **Registration**: Allows requests from the REGISTERED (and authenticated) address; otherwise LifeSize Transit authenticates. **None**: No requests are authenticated.
Trusted hosts	Adds a set of hostnames/IP addresses (with optional SIP port) for the trusted hosts. These are not challenged for authentication and require a database user entry. An example is an MCU registering conferences.
Proxy Mode	The proxy mode affects the routing between SIP users on external hosts or other servers. External requests can be handled by redirect or forward. The default is **Forward**.

Registered SIP Users

This page contains a table that lists all SIP users registered in the built-in registrar, with information about their contact address, registration and expiry times. Proxy registrations (registrations through Transit Server belonging to a third-party registrar) are also shown in the Connected Clients table.

Label	Description
SIP URI	The registered SIP user ID.
Alias	An optional second identifier per user, typically used for incoming calls from the PSTN.
Expires	The lifetime of this expiry. If the client does not register again before this time, it will be unregistered.
Contact	The IP address and port on which the client is registered as reported in the contact header.
Unregister	Clears the registration. The client will still believe that it is registered, but will not receive any calls. This does not prevent the user from registering again.

SIP Routing

The **SIP Routing** page contains routing configuration settings for SIP calls.

Label	Description
Domain Routing	Allows the operator to specify routing to SIP overriding the default DNS lookups. The routing operation is performed on SIP domains (for example, `example.com` with users *`user`*`@example.com`).
Domain	Specifies the SIP domain for the routing entry. Requests to users with this domain will be sent to the addresses specified in the **SIP Host** column.
SIP Host	Specifies the SIP destination for the domain. By default, SIP requests are routed to the domain in the SIP-URI after a SIP SRV DNS lookup. When testing or using SIP servers that are not routable through SIP SRV DNS, the domains and IP addresses can be specified in this field. LifeSize Transit Server does not perform SRV DNS lookups for these domains; requests are routed directly to the addresses (if numeric IP addresses, otherwise a host lookup is performed). You can configure more than one host per domain, separated with commas. The additional hosts will only be used as backup if the primary host is not responding. Each host can also have a `;transport=udp/tcp` to enforce a particular transport, on this form: `1.2.3.4:5080;transport=tcp,5.6.7.8:5060;transport=udp`
Tunnel via	Reserved for future use.

Label	Description
Routing Phone Numbers	**Routing Phone Numbers** The LifeSize Transit Server registrar includes an expression-based scheme for resolving a phone number to a SIP-URI. It treats an incoming call as a phone number call if the request-URI is a TEL: URI or a SIP URI where the user part of the URI is only digits (including dash -, plus +, star *, and pound #) and the user=phone parameter is present, or the domain part is a local domain for this registrar or this server's local IP address. If the number matches the configured local prefixes it is considered a local number and the registrar looks it up in the database. Otherwise, the matching expressions are queried for a match in case the corresponding result expression is executed to resolve it to a SIP-URI. The expression rules consist of one matching expression and one result expression, resolving to a SIP-URI (the string is implicitly added to the output). They are based on shell expressions (not regular expressions), including wildcards for digits to be removed, and optionally to be included in the result. The order of the rules is significant; more general rules can eclipse more specific rules so place the most specific first. The matching expression can include digits, + (international), plus the wildcard question mark (?) and star (*). The question mark (?) is exactly one wildcard digit and will not be part of the output. The star (*) matches one or more digits (not zero). If the star (*) is part of the result string, the matches are placed in output. Any character after the star (*) in the number expression has no meaning. The first star (*) encompasses all further digits. The star (*) can be placed anywhere in the result expression. Dashes (-) are considered insignificant and are removed from number AND expressions. The international plus sign (+) is regarded as a matching digit (+44* does not match 44*), but can only be present first in number or output expressions. The result expression can hold all characters, where only the star (*) has special meaning. It must end with a hostname. If you specify home routing on the **SIP Configuration** page, the expressions are not queried for calls from non-local users to a number, but are routed to the home of the calling user.

Label	Description
Testing	For convenient testing of expressions, you can enter a number and see what it resolves to by pressing the Test button.
ENUM queries	If no match was found in the expressions for a number, the LifeSize Transit Server can optionally perform an ENUM query to resolve the number to a SIP URI. This checkbox allows or disallows the ENUM queries.

Event Reporting

Refer to ”Troubleshooting” on page 47.

Call Status

”Troubleshooting” on page 47.

H.323 Configuration

The H.323 Configuration page contains configuration settings for H.323.

Field	Description
Gatekeeper mode	Selects between built in, a gatekeeper on the private LAN, and a publicly available external H.323 Gatekeeper. If you select the gatekeeper at private LAN you will also need to configure a route to this gatekeeper on the H.323 Routing page. Refer to ”H.323 Routing” on page 67.
Gatekeeper ID	Specifies the ID for the built-in gatekeeper. Available only if gatekeeper mode is set to **Use built-in gatekeeper**.
Gatekeeper Address	Specifies an external gatekeeper. Available only if gatekeeper mode is set to **Use external gatekeeper**.
Vendor	The vendor of the gatekeeper. Available only if gatekeeper mode is set to **Use external gatekeeper**.

Field	Description
RAS Authentication	Authentication mode for selected RAS messages. The mode can be one of the following: **None**: No authentication **Alias**: H.323 ID/Alias in H.323 messages must match previously provisioned user ID. **Prefix**: H.323 ID/Alias in H.323 messages must start with one of the prefixes configured on this page. If H.323 email ID is present in the H.323 messages then meaning is reversed and it must end with one of the prefixes configured on this page. **CAT/MD5**: Valid Cisco Access Token or digital digest of user ID and password must be present in H.323 message. Authentication mode is applied regardless of whether an external or built in gatekeeper is used.
Q931 Authentication	Authentication mode for Q.931/Setup message. Authentication types are the same as for RAS.
Prefixes for prefix authentication separated by |:	Defines the set of prefixes that are allowed to register and/or make calls. Incoming RAS/Q931 messages must have H.323 Alias or Number that starts with one of these prefixes. Available only when RAS and/or Q931 Authentication mode is set to “Prefix.”
Connected H.323 backend servers	Always 1 for Transit deployments.

H.323 Routing

Similar to SIP, H.323 routes can be manually configured when using the built-in gatekeeper or a gatekeeper in the private LAN. If using an external gatekeeper, neighbor servers should be configured on this. There is no default DNS based location method for H.323 servers, so configuring the routes for inter-domain is even more important with H.323. An H.323 route is identified with a domain (the domain of email-IDs or email-style H.323IDs) or a number prefix (the initial digits of a phone number).

Field	Description
H.323 Prefix or Domain	The domain, or prefix, of a neighbor H.323 server. Use Zone Prefix “*” to add a default gatekeeper. Location Requests will be sent to the default gatekeeper in case no zone prefix match is found.

Field	Description
H.323 Zone Gatekeeper host[:port]:	Insert the address (optionally:port) of the gatekeeper. Multiple gatekeeper addresses can be set up for redundancy, separated with commas
Tunnel via	Use this field to set up a route to a LAN deployed H.323 gatekeeper. Enter the user ID of LifeSize Transit Client. H.323 messages to this domain will be routed to this client, which forwards it to the gatekeeper. The gatekeeper host is in this case the address of the internal gatekeeper. The server must be set up to use gatekeeper on private LAN if you plan to use this option.
Vendor	Select the vendor. If the gatekeeper vendor is none of those, select Radvision.

Logging

The **Log Management** page enables you to control and view the LifeSize Transit logging mechanism. You can also download the current log files for simple viewing. Consult LifeSize Technical Services if you need assistance with logging.

Field	Description
Level of logged messages	Choose the level of information to log and then push the *Set* button. A fine log level increases CPU usage; LifeSize recommends you do not change the default setting.
Select the log groups to exclude	Choose *All*, *None* or desired log groups (possible by toggling on/off desired log groups) and then push the *Apply* button.
Presets	Allows you to store current logging settings, in case you need to restore them later.
Current log files	To inspect a log file, download either the original file or a zipped version (useful on slow connections) by clicking the appropriate link. The most recent file is the one with the lowest index.

Software Upgrade

Refer to ”Upgrading Software” on page 47.

Additional Maintenance Tasks

Refer to the following:

- ”Database Backup and Restore” on page 46.
- ”Troubleshooting” on page 47 for information about creating a diagnostic file.

Appendix B: LifeSize Transit Client Configuration Settings

Several LifeSize Transit configuration settings are preconfigured in the **Operation & Maintenance** user interface. Unless specifically instructed in the deployment scenarios described in this guide or by LifeSize Technical Service representatives, LifeSize recommends that you do not change them. The following tables describe these settings for LifeSize Transit Client and are for reference only. Consult LifeSize Technical Services if you need assistance modifying your configuration. Refer to ”Appendix A: LifeSize Transit Server Configuration Settings” on page 55 for information about configuration settings for LifeSize Transit Server.

Current Status Page

The Current Status page appears when you access the LifeSize Transit Client web administration interface.

Field	Description
Status	Status codes are one of the following: **NotRunning** LifeSize Transit Client is not running. **Idle** LifeSize Transit Client has not set up a tunnel because the firewall supports UDP. **Connecting** LifeSize Transit Client is trying to connect to LifeSize Transit Server. **Connected** LifeSize Transit Client is connected to LifeSize Transit Server. **Disabled** An error occurred which prevents LifeSize Transit Client from connecting to LifeSize Transit Server.

Field	Description
Network	As a result of STUN (RFC 3489) detection, LifeSize Transit Client has detected that it is behind one of the following types of firewall/NATs: **UdpBlocked** The firewall/NAT router does not allow UDP. Tunnelling must be used. **OpenInternet** There is no firewall/NAT router. Direct UDP connections can be used. **FullConeNAT** **RestrictedNat** **PortRestrictedNat** The firewall/NAT router allows UDP. LifeSize Transit will use direct or relayed UDP connections for registrations and calls, depending on the peer in a call. **SymmetricNat** **SymmetricUdpFirewall** The firewall/NAT router allows UDP, but media must be relayed through a public host. LifeSize Transit will use relayed UDP for media.
Current Registrations	The number of current registrations on LifeSize Transit Client.
Current Calls	The number of calls in progress on LifeSize Transit Client.
Version	The software version of LifeSize Transit Client.

Registered Users

This page shows the current registered clients on LifeSize Transit Client.

Field	Description
UserID	The user ID of the registered user.
Address	The address from which the user registered.
Protocol	The protocol (for example, SIP or H.323) used by the registered user.

Field	Description
Mode	The mode of registration towards LifeSize Transit Server. Can be UDP if the firewall allows UDP out to the server and the LifeSize Transit Client works as a standard SIP proxy, TCP if SIP over TCP is used towards the server, or Tunneled if LifeSize Transit Client has a tunnelled connection for this registration. You can specify this mode in the SIP Settings page. Refer to ”SIP Settings” on page 74.
TTL	The time-to-live on the registration, in seconds. If the user does not register again before this time lapses, the registration is cleared.
ClientType	The type of SIP/H.323 client. This is free-text field from the registered client for SIP and a product ID field (if present) of the device vendor of the registered client for H.323 calls.

Current Calls

This page shows the current calls on LifeSize Transit Client.

Calls where both the calling and the called party are registered through LifeSize Transit Client are shown as two calls, even if the media is passed directly on the local network.

Field	Description
Caller	The user ID of the calling user. The word **local** appears in parenthesis after the user ID if this user is connected through the LifeSize Transit Client. If both the caller and the callee in the call are local, two calls are shown with only one local user identified in each call.
Callee	The user ID of the called user. The word **local** appears in parenthesis after the user ID if this user is connected through LifeSize Transit Client. If both the caller and the callee in the call are local, two calls are shown with only one local user identified in each call.
Call-ID	The call ID that identifies this call uniquely.

Field	Description
MediaMethod	One of the following types of media connection methods in use for this leg of the call: **Direct**: Media is flowing directly between the callers. They are either on the same local network, or the firewall allows unhindered UDP traffic. **Relayed**: Media is relayed by UDP through LifeSize Transit Server. **Tunnelled**: Media is tunnelled over HTTPS or TCP to LifeSize Transit Server. **H.460.19**: The H.323 calls use H.460.19 media multiplexing and traversal. **STUN**: Media is using STUN for direct media transmission through NAT. **TURN**: Media is sent using TURN towards a TURN server for relaying media. **ICE**: Media is using ICE to dynamically negotiate the most efficient path.
Streams	A list of the types of media streams in the call. If more than one type exists, the types are separated by the / character. These are freeform strings.
State	The call state. Frequently used call states include the following: **Reserving**: Media resources are being reserved. **Proceeding**: Contacting the called party, but that party has not answered yet. **Active**: The call is established, media is flowing. **Cancelling**: The calling party is hanging up. **Ending**: The call is ending.

Connection

Use this page to modify connection details.

Note: Changing these settings terminates calls in progress.

Field	Description
UserID	The user ID and password to authenticate towards LifeSize Transit Server. This user ID and password is for LifeSize Transit Client and works for all devices connecting through LifeSize Transit Client.
LifeSize Transit Servers	The LifeSize Transit Server to which the LifeSize Transit Client connects.

SIP Settings

Use this page to modify SIP settings..

Field	Description
Current SIP UDP/TCP port	The SIP port used to communicate with the clients on the local network, using UDP or TCP. The default is 5060. If you modify this, the new value must be propagated to the clients. If LifeSize Transit Client fails to grab the new port (for example, if there is another application on the host holding the new port), the old port is used.
Current SIP TLS port	This feature is not supported.
Signaling Mode	Controls the signalling mode towards LifeSize Transit Server. **Auto**: This is the default setting, where LifeSize Transit Client detects the optimal signalling mode. If the network probing detected that UDP is allowed through the firewall, UDP will be used if the SIP messages do not exceed the maximum IP packet size on the network. In this case, TCP is used on a per message basis. If TCP cannot be used, a tunnel connection is set up for signalling. **UDP**: Always uses UDP for SIP transport to the server. **TCP**: Always uses TCP for SIP transport to the server. **TLS**: Always uses TLS for SIP transport to the server. **Tunnelled**: Always establishes a tunnelled connection to the LifeSize Transit Server.
SIP/TLS Trusted Root Certificates	This feature is not supported.

H.323 Settings

Use this page to modify H.323 settings..

Field	Description
Current H.225 port	The TCP port to bind to for H.225.0 call signalling. It is automatically passed to registering H.323 endpoints and gatekeepers using Location Requests. It may need to be provisioned on a LAN deployed gatekeeper if it passes SETUP on directly, without initial Location Requests. The default is 2222.

Field	Description
Current RAS port	The UDP port to bind to for RAS signalling, among others used for registration. The default is 1719. If using a non-standard port this must be provisioned as the gatekeeper port on the H.323 endpoints before registration.
H460.18/19 Traversal Server	Sets the address and RAS port of a H.460.18/.19 server. It also controls the H.323 signalling mode towards the server. If this server address is empty (the default), H.323 signalling will be done over a TCP tunnel to the server. If it is not empty, H.460.18/.19 is used. If you configured LifeSize Transit Server to use a gatekeeper in the private LAN, this field is not available and the TCP tunnel is used. For other gatekeeper configuration options either a TCP tunnel or the H.460.18/19 traversal server can be used. To use the H.460.18/19 traversal server, enter the IP address of the LifeSize Transit signalling server.
Internal Gatekeeper Address	The address of the gatekeeper that is in the private LAN when this option is selected and an H.323 routing entry is configured for LifeSize Transit Server. This field is automatically populated from LifeSize Transit Server.
Outbound prefix at Gatekeeper	Prefix for outbound calls when using a gatekeeper in the private LAN with LifeSize Transit Server.
Strip prefix from outbound calls	When selected, LifeSize Transit Client strips the outbound prefix in the dial string when it is included in an outbound call.
Register at Gatekeeper	Selecting this option and then clicking **Set** registers LifeSize Transit Client with the gatekeeper in the private LAN and enables outbound calls to be forwarded to LifeSize Transit Client.
Registration status	Indicates the status of LifeSize Transit Client's registration to the gatekeeper. The status can be one of the following: • Registered • Registering (the gatekeeper is not available) • Not registered (awaiting the gatekeeper address; the gatekeeper IP address is not populated from LifeSize Transit Server; or the Register at Gatekeeper option has been cleared)

Media Transport

Settings on this page control the traversal methods used for calls.

Field	Description
Media Tunnel Mode	When set to **Auto**, LifeSize Transit Client automatically selects the optimal transport. When set to **Always**, all media is tunnelled to LifeSize Transit Server. This may be needed in special cases, for example, if you require all calls to be transported securely over HTTPS.
Media Transports	
Enable ICE (SIP only)	Enables ICE for SIP calls. ICE is a protocol embedded in SIP/SDP that lets the parties of a call dynamically detect the optimal traversal method. ICE is only used between peers. It is backwards compatible with non-ICE supporting SIP devices, but implementations rejecting a call with the ICE extensions are possible. If that occurs, consider disabling ICE.
Enable STUN	Enables the use of STUN within an ICE session, or on UDP friendly networks. STUN lets a client detect its public address to be advertised in a call so the media can go without relay on UDP friendly networks. **Override STUN Servers**: If you wish to specify a STUN server other than LifeSize Transit Server, enter the address here. More than one server can be configured (space separated, possibly with *:port*).
Enable TURN	When checked, enables use of TURN; a standard relay method. The LifeSize Transit client uses this if no control tunnel is established and peer-to-peer media is not possible, or within an ICE session. If a control tunnel is established, the LifeSize Transit proprietary scheme will be used instead, as it traverses more difficult networks by tunnelling over HTTPS and utilizing web proxies if needed. **Override TURN Servers**: If you wish to use a TURN server other than LifeSize Transit Server, enter the address here. More than one server can be configured (space separated, possibly with *:port*).

Logging

Use this page to control the level of details that are sent to the log and to download the current log files for simple viewing.

Field	Description
Level of Logging	Choose the desired log level from one of the following and then click **Set**: • **Severe**: Only malfunctions that severely affect system behavior, such as connection failures, bad passwords are logged. • **Warning**: As above, plus that unexpected behavior such as badly formatted SIP messages are logged. • **Main**: As above, plus that major system events are logged, such as registrations and calls. • **Info**: A more detailed view of operation. Most SIP messages and Interworking are logged. • **Debug**: Full logging. Using this level affects system performance. Use this level only when investigating a problem.
Select log file to download	Click a log file filename to download the file for simple viewing.

Upgrade

Refer to ”Upgrading Software” on page 47.

Diagnostics

Refer to ”Troubleshooting” on page 47.

Configuration

The Configuration page contains the product serial number and a reboot button for rebooting LifeSize Transit Client.